Ekwan E. Rhow - State Bar No. 174604
Dorothy Wolpert - State Bar No. 73213
Thomas R. Freeman - State Bar No. 135392
Marc E. Masters - State Bar No. 208375
mmasters@birdmarella.com
BIRD, MARELLA, BOXER, WOLPERT, NESSIM, DROOKS, LINCENBERG & RHOW, P.C.
1875 Century Park East, 23rd Floor
Los Angeles, California 90067-2561
Telephone: (310) 201-2100
Facsimile: (310) 201-2110

Attorneys for Plaintiffs Misty Hong, minor A.S., through her mother and legal guardian Laurel Slothower, and minor A.R., through her mother and legal guardian Gilda Avila

[Additional Counsel on Signature Page]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

MISTY HONG, minor A.S., through her mother and legal guardian LAUREL SLOTHOWER, minor A.R., through her mother and legal guardian GILDA AVILA, MEGHAN SMITH, minors C.W. and I.W., through their mother and legal guardian MIKHAILA WOODALL, and minor R.P., through her mother and legal guardian LYNN PAVALON individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

BYTEDANCE, INC., a corporation, TIKTOK, INC., a corporation; BEIJING BYTEDANCE TECHNOLOGY CO. LTD,, a privately-held company; and MUSICAL.LY, a corporation.

Defendants.

CASE NO. 5:19-cv-07792-LHK

Hon. Lucy H. Koh

FIRST AMENDED CLASS ACTION COMPLAINT FOR:

(1) Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030
(2) Violation of the California Comprehensive Data Access and Fraud Act, Cal. Pen. C. § 502
(3) Violation of the Right to Privacy - California Constitution
(4) Intrusion upon Seclusion
(5) Violation of the California Unfair Competition Law, Bus. & Prof. C. §§ 17200 *et seq.*
(6) Violation of the California False Advertising Law, Bus. & Prof. C. §§ 17500 *et seq.*
(7) Negligence
(8) Restitution / Unjust Enrichment
(9) Violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.*

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

I. INTRODUCTION.

1. TikTok is one of the most popular entertainment apps for mobile devices in the United States. It has acquired one of the largest installed user bases in the country on the strength of its popular 15-second videos of fun activities like dancing, lip-syncing, and stunts. Unknown to its users, however, the TikTok app also includes China-based surveillance software. The TikTok app clandestinely has vacuumed up and transferred to servers in China (and to other servers accessible from within China) vast quantities of private and personally-identifiable user data and content that can be employed to identify, profile and track the physical and digital location and activities of United States users now and in the future.

2. The TikTok app also surreptitiously has taken TikTok users' private draft videos they never intended for publication – without notice or consent. Defendants and their sophisticated China-based engineering team covertly mine these private videos, as well as publicly posted TikTok user videos, for highly sensitive and immutable biometric identifiers and information. In addition to this mining of TikTok user videos at the server level in China, the functionality and code of the TikTok app itself evidences Defendants' collection and use of TikTok users' biometric identifiers and information – again without notice or consent.

3. In short, the TikTok app's lighthearted fun comes at a heavy cost. Meanwhile, Defendants unjustly profit from the secret harvesting of this massive array of private and personally-identifiable TikTok user data and content by using it for targeted advertising, improvements to Defendants' artificial intelligence technologies, the filing of patent applications, and the development of consumer demand for, and use of, Defendants' other products. Defendants' conduct violates statutory, constitutional, and common law privacy, data, biometrics and consumer protections, and it should be stopped.

II. THE PARTIES.

A. The Plaintiffs.

4. Plaintiff Misty Hong is, and at all relevant times was, an individual and

resident of Palo Alto, California.

5. Plaintiff A.S., a minor, is, and at all relevant times was, an individual and resident of Stevenson Ranch, California. A.S. brings this suit by and through her mother and legal guardian, Laurel Slothower, who is, and at all relevant times was, an individual and resident of Stevenson Ranch, California.

6. Plaintiff A.R., a minor, is, and at all relevant times was, an individual and resident of Pasadena, California. A.R. brings this suit by and through her mother and legal guardian, Gilda Avila, who is, and at all relevant times was, an individual and resident of Pasadena, California.[1]

7. Plaintiff Meghan Smith is, and at all relevant times was, an individual and resident of Champagne, Illinois.

8. Plaintiffs C.W., a minor, and I.W., a minor, are, and at all relevant times were, individuals and residents of Chicago, Illinois. C.W. and I.W. bring this suit by and through their mother and legal guardian, Mikhaila Woodall, who is, and at all relevant times was, an individual and resident of Chicago, Illinois.

9. Plaintiff R.P., a minor, is, and at all relevant times was, an individual and resident of Chicago, Illinois. R.P. brings this suit by and through her mother and legal guardian, Lynn Pavalon, who is, and at all relevant times was, an individual and resident of Chicago, Illinois.[2]

B. The Defendants.

10. Defendant ByteDance, Inc. is, and at all relevant times was, a Delaware corporation with its principal place of business in Palo Alto, California. Defendant ByteDance, Inc. is a wholly-owned subsidiary of ByteDance, Ltd., a Cayman Islands corporation.

---

[1] Plaintiffs Misty Hong, A.S. and A.R. are collectively referred to as the "California Plaintiffs."

[2] Plaintiffs Meghan Smith, C.W., I.W. and R.P. are collectively referred to as the "Illinois Plaintiffs." The California Plaintiffs and the Illinois Plaintiffs are collectively referred to as the "Plaintiffs."

11. Defendant TikTok, Inc. f/k/a Musical.ly, Inc. ("TikTok, Inc.") is, and at all relevant times was, a California corporation with its principal place of business in Culver City, California.[3] Defendant TikTok, Inc. also maintains offices in Palo Alto, California and Mountain View, California.[4] The name change from Musical.ly, Inc. to TikTok, Inc. occurred in May 2019. Defendant TikTok, Inc. is a wholly-owned subsidiary of TikTok, LLC, which in turn is a wholly-owned subsidiary of TikTok, Ltd. And TikTok, Ltd. – like Defendant ByteDance, Inc. – is a wholly owned subsidiary of ByteDance, Ltd.

12. Defendant Musical.ly n/k/a TikTok, Ltd. is, and at all relevant times was, a Cayman Island corporation with its principal place of business in Shanghai, China. Defendant Musical.ly was the parent company of Musical.ly, Inc. Defendant Musical.ly changed its name to TikTok, Ltd. and, as noted above, is a wholly-owned subsidiary of ByteDance, Ltd.

13. Defendant Beijing ByteDance Technology Co. Ltd. ("Beijing ByteDance") is, and at all relevant times was, a privately held company headquartered in Beijing, China. Defendant Beijing ByteDance is a wholly-owned subsidiary of ByteDance Co., Ltd., which is also headquartered in Beijing, China. ByteDance Co., Ltd. is owned by founder Zhang Yiming (98.8%) and Zhang Lidong (1.2%). Defendant Beijing ByteDance and ByteDance Co., Ltd. operate as one company.

14. ByteDance, Ltd. owns 100% of ByteDance (HK) Co., Ltd., which is headquartered in Hong Kong. ByteDance (HK) Co., Ltd. in turn owns 100% of Beijing ByteDance Network Technology Co., Ltd., which is headquartered in Beijing, China.

C. Alter Ego And Single Enterprise Allegations.

15. At all relevant times, Defendants TikTok, Inc. and ByteDance, Inc. have

---

[3] https://www.cnbc.com/2019/10/14/tiktok-has-mountain-view-office-near-facebook-poaching-employees.html.

[4] https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-views-about-censorship-often-were-overridden-by-chinese-bosses/; https://www.cnbc.com/2019/10/14/tiktok-has-mountain-view-office-near-facebook-poaching-employees.html.

shared offices in Silicon Valley[5] and also have shared employees. U.S. and China-based employees of the ByteDance family of companies perform work on and concerning the TikTok app that is at the center of this lawsuit, including the functionality and operation of the TikTok app and the Chinese version of the app ("Douyin") that Defendant Beijing ByteDance operates in China. One Director of Engineering in the Mountain View office leads an "augmented reality" team that is tasked with transforming state-of-the-art artificial intelligence and augmented reality technologies into fun features and creative tools for both the TikTok and Douyin apps.

16. At all relevant times, Defendant Beijing ByteDance has directed the operations of Defendants TikTok, Inc. and ByteDance, Inc. with respect to the TikTok app, and Defendants TikTok, Inc. and ByteDance, Inc. have reported to Defendant Beijing ByteDance. In fact, at all relevant times, Defendant Beijing ByteDance has collected and analyzed data from the United States regarding the performance of various features of the TikTok app, and has worked with Defendants TikTok, Inc. and Defendant ByteDance, Inc. to address performance issues. Additionally, at all relevant times, Defendant Beijing ByteDance and its engineers have done significant coding for the TikTok app and its many versions and updates.

17. At certain relevant times, with respect to Defendants' monitoring and censorship of content on the TikTok app, management in China has determined content review policies enforced in Defendant TikTok, Inc.'s Culver City office; a content review manager in the same Culver City office was reporting to someone in China; and another content reviewer was required to seek authorization from someone in China in order to access non-published information about user accounts when content concerns arose. Also, at certain relevant times Defendant Beijing ByteDance employed a vast number of content reviewers in China to review TikTok videos uploaded by United States users, and these

[5] In addition to ByteDance-TikTok cross-listed personnel in Palo Alto, TikTok logos and paraphernalia are found in the ByteDance, Inc. Palo Alto office. *See* https://www.youtube.com/watch?v=RymGJG0miv0.

reviewers in China had authority to take down any such videos if the content was deemed inappropriate or illegal.

18. These facts are consistent with public reporting. For example, "[m]ultiple TikTok sources, who spoke with *The Intercept* on the condition of anonymity …, emphasized the primacy of ByteDance's Beijing HQ over the global TikTok operation, explaining that their ever-shifting decisions about what's censored and what's boosted are dictated by Chinese staff, whose policy declarations are then filtered around TikTok's 12 global offices, translated into rough English, finally settling into a muddle of Beijing authoritarianism crossed with the usual Silicon Valley prudishness."[6]

19. At certain relevant times, Defendant Beijing ByteDance employees have collected TikTok users' feedback regarding upgraded and/or newly-introduced features, and the departments responsible for managing and monitoring TikTok user experience have been based in China. At certain relevant times, employees in these departments reported to their supervisors in China, who in turn shared their findings with Defendant TikTok, Inc. in the United States. At certain relevant times, Defendant Beijing ByteDance employees also distributed questionnaires to TikTok users, and collected and recorded reports from such users about problems they were experiencing. At certain relevant times, employees in the United States contacted TikTok users, and took notes regarding such users' experiences. At certain relevant times, these notes were translated into Chinese and sent to Defendant Beijing ByteDance executives to review and analyze.

20. At certain relevant times, Defendant Beijing ByteDance made key strategy decisions for Defendants TikTok, Inc. and ByteDance, Inc., as well as for offices elsewhere in the world, and Defendants TikTok, Inc., ByteDance, Inc. and the other offices were tasked with executing such decisions. A publicly-available interview of Isaac Bess and Gregory Justice on YouTube is consistent with these facts. In that interview, Isaac Bess identifies himself as responsible for leading "ByteDance" business development from

[6] https://theintercept.com/2020/03/16/tiktok-app-moderators-users-discrimination/.

Los Angeles, and Gregory Justice identifies himself as part of Defendant TikTok, Inc.'s content team in Los Angeles. Both discuss having regular all-hands bi-monthly meetings with the CEO in China to discuss global strategy with the "local teams."[7]

21. At all relevant times, and in connection with the matters alleged herein, each Defendant acted as an agent, servant, partner, joint venturer and/or alter ego of each of the other Defendants, and acted in the course and scope of such agency, partnership, and relationship and/or in furtherance of such joint venture. Each Defendant acted with the knowledge and consent of each of the other Defendants and/or directed, authorized, affirmed, consented to, ratified, encouraged, approved, adopted, and/or participated in the acts or transactions of the other Defendants.

22. At all relevant times, and in connection with the matters alleged herein, Defendants were controlled and largely-owned by the same person, founder Zhang Yiming, and constitute a single enterprise with a unity of interest. Recognition of the privilege of separate existence under such circumstances would promote injustice.

III. JURISDICTION AND VENUE.

23. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) & 1367 because: (i) this is a class action in which the matter in controversy exceeds the sum of $5,000,000, exclusive of interest and costs; (ii) there are 100 or more class members; and (iii) some members of the class are citizens of states different from some Defendants, and also because two Defendants are citizens or subjects of a foreign state.

24. This Court has personal jurisdiction over Defendants because: (i) they transact business in the United States, including in this District; (ii) they have substantial aggregate contacts with the United States, including in this District; (iii) they engaged and are engaging in conduct that has and had a direct, substantial, reasonably foreseeable, and intended effect of causing injury to persons throughout the United States, including in this

[7] https://www.youtube.com/watch?v=lKV6wsdI4-A (at 0:20 – 0:54; 15:59 – 17:08).

District, and purposely availed themselves of the laws of the United States.

25. In accordance with 28 U.S.C. § 1391, venue is proper in this District because: (i) a substantial part of the conduct giving rise to the claims occurred in and/or emanated from this District; (ii) Defendants transact business in this District; (iii) one Defendant has its principal place of business in this District; (iv) two Defendants have offices in this District; and (v) Plaintiff Misty Hong resides in this District.

IV. THE RISE OF DEFENDANTS AND THEIR DANGEROUS APPS.

A. Defendant Beijing ByteDance Becomes A China-Based Tech Giant Focused On Overseas Markets, Particularly In The United States.

26. Defendant Beijing ByteDance was founded in 2012 and makes a variety of video and news-aggregation apps.[8] It "regards its platforms as part of an artificial intelligence company powered by algorithms that 'learn' each user's interests and preferences through repeat interaction."[9] Because Defendant Beijing ByteDance emerged only after other China-based tech giants had taken over the market in China, Defendant Beijing ByteDance has looked to overseas markets, including those in the United States, for growth.[10]

27. Defendant Beijing ByteDance had $7.2 billion in annual revenue for the year 2018. It far surpassed this number in 2019, booking $7 billion to $8.4 billion in revenue in a better-than-expected result for the first half of 2019.[11] Defendant Beijing ByteDance currently is worth between $75 billion and $78 billion.[12] Investors in Defendant Beijing

---

[8] https://www.wsj.com/articles/tiktoks-videos-are-goofy-its-strategy-to-dominate-social-media-is-serious-11561780861.

[9] https://www.law360.com/articles/1213180/sens-want-tiktok-investigated-for-national-security-threats; https://www.cotton.senate.gov/?p=press_release&id=1239.

[10] https://www.wsj.com/articles/tiktoks-videos-are-goofy-its-strategy-to-dominate-social-media-is-serious-11561780861.

[11] https://www.cnbc.com/2019/09/30/tiktok-owner-bytedances-first-half-revenue-better-than-expected-at-over-7-billion-sources.html.

[12] https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-

ByteDance include Sequoia Capital China, Russian billionaire Yuri Milner, Japanese technology giant SoftBank, and big private-equity firms such as KKR, General Atlantic, and Hillhouse Capital Group.[13]

28. Most of Defendant Beijing ByteDance's revenue is generated from advertising.[14] "ByteDance has [] been doubling down on its advertising business as the company's management sets increasingly ambitious revenue goals."[15] "As with pretty much all major social media and content startups, ByteDance monetises through advertising. Specifically, it runs targeted advertising within user feeds – providing them promotional content in between using the app."[16]

B. The Musical.ly App Evolves Into The TikTok App.

29. Defendant Musical.ly (named, and now known as, TikTok, Ltd.) and Defendant Musical.ly, Inc. (named, and now known as, TikTok, Inc.) launched the highly-popular social media and social networking app "Muscial.ly" in 2014. This app allows its users to (i) create video selfies of themselves dancing and/or lip-syncing with a musical soundtrack in the background, and (ii) share such videos with friends.[17] There are simple tools provided by the Musical.ly app that users can utilize to create and edit these videos, and the app provides a large online music library from which users may select their background music. The Musical.ly app was designed "to capture the YouTube phenomenon of teenagers sharing videos of themselves singing or dancing to popular

views-about-censorship-often-were-overridden-by-chinese-bosses/; https://www.reuters.com/article/us-tiktok-cfius-exclusive/exclusive-us-opens-national-security-investigation-into-tiktok-sources-idUSKBN1XB4IL.

[13] https://www.wsj.com/articles/lip-syncing-app-musical-ly-is-acquired-for-as-much-as-1-billion-1510278123; https://www.reuters.com/article/us-tiktok-cfius-exclusive/exclusive-us-opens-national-security-investigation-into-tiktok-sources-idUSKBN1XB4IL.

[14] https://www.bloomberg.com/news/articles/2019-01-15/bytedance-is-said-to-hit-lower-end-of-sales-goal-amid-slowdown.

[15] https://technode.com/2019/09/20/bytedance-launches-video-ad-tools-for-tiktok-douyin/.

[16] https://www.businessofapps.com/insights/bytedance-social-media-advertising-company/.

[17] https://www.wsj.com/articles/lip-syncing-app-musical-ly-is-acquired-for-as-much-as-1-billion-1510278123.

music."[18] Beyond the creation and sharing of videos, the Musical.ly app provides a platform through which users can interact, including by commenting on other users' videos and "following" other users' accounts. Users also can send direct messages in order to communicate with other users on the app. By November 2017, the Musical.ly app had 60 million monthly active users.[19]

30. Meanwhile, in 2016, Defendant Beijing ByteDance launched its own app called "Douyin" in China, which mimicked the Musical.ly app.[20] By 2017, shortly before its purchase of Defendants Musical.ly and Musical.ly, Inc., Defendant Beijing ByteDance introduced an English-language version of the Douyin app outside China under the name "TikTok." In August 2018, after having acquired Defendants Musical.ly and Musical.ly, Inc., Defendant Beijing ByteDance combined the Musical.ly app with its TikTok app, merging all existing accounts and data into a single app under the retained "TikTok" name.[21]

31. The Musical.ly and TikTok apps are hereafter collectively referred to as the "TikTok app," and the Musical.ly and TikTok users are hereafter collectively referred to as the "TikTok users."

C. The TikTok App Becomes A Global Phenomenon With A Strong Presence In The United States.

32. The TikTok app has become "one of the world's fastest-growing social media platforms" and a "global phenomenon" with a massive American audience.[22] In

---

[18] https://www.wsj.com/articles/lip-syncing-app-musical-ly-is-acquired-for-as-much-as-1-billion-1510278123.

[19] https://www.wsj.com/articles/lip-syncing-app-musical-ly-is-acquired-for-as-much-as-1-billion-1510278123; https://www.nytimes.com/2019/11/01/technology/tiktok-national-security-review.html.

[20] https://www.wsj.com/articles/tiktoks-videos-are-goofy-its-strategy-to-dominate-social-media-is-serious-11561780861.

[21] http://culture.affinitymagazine.us/tik-tok-is-scamming-people-stealing-information/.

[22] https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-

November 2019, the *Washington Post* reported that the TikTok app had been downloaded more than 1.3 billion times worldwide, and more than 120 million times in the United States.[23] However, by April 2020, *TechCrunch* reported that the TikTok app's worldwide downloads already had surpassed 2 billion, and that in "the quarter that ended on March 31, TikTok was downloaded 315 million times — the highest number of downloads for any app in a quarter."[24] It is the most downloaded non-game app in the world.[25] The TikTok app routinely outranks its top competitors – such as Facebook, Snapchat, and Instagram – on the Apple and Google app stores.[26] In fact, it has been the most downloaded app on the Apple and Google app stores for months.[27] As of August 2019, the TikTok and Douyin apps had 625 million monthly active users.[28] The average user opened the TikTok app more than 8 times per day and spent approximately 45 minutes on the app daily as of March 2019.[29]

33. In January 2020, *Barron's* reported on the TikTok app's revenue: "The wildly popular short-video service generated $176.9 million in revenue in 2019—71% of the total $247.6 million in revenue the app has ever generated, according to new data from the app-tracking firm SensorTower. In the fourth quarter alone, TikTok had revenue of $88.5 million, up two times from the third quarter and up six times year over year, most of that from advertising and in-app purchases, SensorTower reports. China accounted for

---

views-about-censorship-often-were-overridden-by-chinese-bosses/.

[23] https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-views-about-censorship-often-were-overridden-by-chinese-bosses/.

[24] https://techcrunch.com/2020/04/29/tiktok-tops-2-billion-downloads/.

[25] https://www.cnbc.com/2019/07/25/china-camera-apps-may-open-up-user-data-to-beijing-government-requests.html.

[26] https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-views-about-censorship-often-were-overridden-by-chinese-bosses/.

[27] https://thehill.com/policy/technology/469114-tiktok-faces-lawmaker-anger-over-china-ties.

[28] https://thehill.com/policy/technology/469114-tiktok-faces-lawmaker-anger-over-china-ties.

[29] https://www.wsj.com/articles/tiktoks-videos-are-goofy-its-strategy-to-dominate-social-media-is-serious-11561780861.

about 69% of the company's 2019 revenue, according to the firm, with U.S. revenues accounting for 20%."[30] Evidencing the TikTok app's rapid growth, three months later, *TechCrunch* reported that: "Users have spent about $456.7 million on TikTok to date, up from $175 million five months ago. Much of this spending — about 72.3% — has happened in China. Users in the United States have spent about $86.5 million on the app, making the nation the second most important market for TikTok from the revenue standpoint."[31]

34. This level of success globally and in the United States is rare for a China-based tech giant. Facebook CEO Mark Zuckerberg acknowledged as much, stating that the TikTok app "is really the first consumer internet product built by one of the Chinese tech giants that is doing quite well around the world. It's starting to do well in the U.S., especially with young folks."[32] Indeed, Defendant TikTok, Inc. recently took over office space in Silicon Valley once occupied by Facebook's WhatsApp messaging app, and is poaching employees from rival Facebook by offering salaries as much as 20% higher.[33] Other competitors from whom Defendant TikTok, Inc. is hiring away employees include Snap, Hulu, Apple, YouTube and Amazon.[34]

35. One key to Defendants' financial success is the targeted advertising that they run through the TikTok app. Such targeted advertising relies heavily upon knowledge of each user's preferences.[35] Through a secretive and highly-invasive information gathering campaign, Defendants have unlawfully accumulated private and personally-identifiable data and content on TikTok users that Defendants are assembling in user profiles or

---

[30] https://www.barrons.com/articles/beware-facebook-tiktok-revenues-are-exploding-51579201752.

[31] https://techcrunch.com/2020/04/29/tiktok-tops-2-billion-downloads/.

[32] https://www.cnbc.com/2019/10/14/tiktok-has-mountain-view-office-near-facebook-poaching-employees.html.

[33] https://www.cnbc.com/2019/10/14/tiktok-has-mountain-view-office-near-facebook-poaching-employees.html.

[34] https://www.cnbc.com/2019/10/14/tiktok-has-mountain-view-office-near-facebook-poaching-employees.html.

[35] https://www.digitaltrends.com/social-media/tiktok-advertiser-audience-network-targeted-ads/.

dossiers and monetizing for the purpose of unjustly profiting from their unlawful activities.

V. DEFENDANTS' THEFT OF PRIVATE AND PERSONALLY-IDENTIFIABLE TIKTOK USER DATA AND CONTENT.

A. Defendants' Secret Taking Of Private TikTok User Videos and TikTok User/Device Identifiers Without Notice Or Consent.

1. Defendants Settle An FTC Lawsuit Alleging They Unlawfully Collected And Used Children's Data.

36. On February 27, 2019, the United States, on behalf of the Federal Trade Commission ("FTC"), filed a lawsuit against Defendants Musical.ly and Musical.ly, Inc. alleging they had violated the Children's Online Privacy Protection Act by collecting and using personal data from children under age 13 without the required notice and consent.[36]

37. On the same date, Defendants Musical.ly and Musical.ly, Inc. stipulated to an order mandating, among other things, a civil penalty in the amount of $5.7 million and injunctive relief concerning the collection and destruction of children's personal data.[37]

38. This is the largest civil penalty ever imposed for such a violation.[38] The FTC also published a statement indicating that, "[i]n our view, these practices reflected the company's willingness to pursue growth even at the expense of endangering children."[39]

2. The TikTok App Secretly Takes Users' Private Videos Before Users Are Given The Choice Whether To Save Or Post Them.

39. Unless shared through the affirmative consent of the TikTok user, videos created using the TikTop app, which often include close-ups of faces and private acts

---

[36] *United States of America v. Musical.ly and Musical.ly, Inc.*, United States District Court, Central District of California, Case No. 2:19-cv-1439.

[37] *United States of America v. Musical.ly and Musical.ly, Inc.*, United States District Court, Central District of California, Case No. 2:19-cv-1439.

[38] https://www.wsj.com/articles/tiktoks-videos-are-goofy-its-strategy-to-dominate-social-media-is-serious-11561780861; https://www.techinasia.com/tiktok-owner-bytedance-gathers-1-billion-monthly-active-users-apps.

[39] https://www.nbcnews.com/tech/tech-news/tiktok-pay-5-7-million-over-alleged-violation-child-privacy-n977186.

unintended for public consumption, are inherently private, personal and sensitive.

40. After using the TikTok app to record a video, a screen presents TikTok users with certain options, including the following: (i) an "x" button; (ii) a "next" button; and (iii) a button for effects. The "x" button takes TikTok users to a screen with options, including "reshoot" and "exit." The "next" button takes TikTok users to a screen with options, including "save" and "post." The "effects" button takes TikTok users to a screen offering the ability to modify the video.

41. Once TikTok users click the "next" button, but before they click either the "save" or "post" buttons, their ***private videos that are neither saved nor posted*** (the "Private Videos") are transferred from their mobile devices to the following domain owned and controlled by Defendants: muscdn.com. The "mus" portion of the domain name stands for Musical.ly, and the "cdn" portion of the domain name stands for content distribution network.

42. During the secret transfer of TikTok users' Private Videos to the domain and servers mentioned above, there is no progress bar or any other indication that their Private Videos are being transferred. Nor is the taking of the Private Videos disclosed in any of Defendants' privacy policies or other disclosure documentation. TikTok users are thus prevented from knowing that Defendants have taken their Private Videos. No user consent exists.

43. This highly invasive breach of TikTok users' privacy is not the only harm that befalls such users as a result of Defendants' theft of their Private Videos. Defendants also take highly sensitive and immutable biometric identifiers and information from these Private Videos, as discussed below, and unjustly profit from such activities.

44. Defendants released a December 2019 version of the TikTok app that transfers five thumbnail images uniformly distributed across each of the Private Videos (the "Private Video Images") to byteoversea.net. The domain byteoversea.net is controlled by Defendants and has numerous sub-domains. Accordingly, when data and content arrives at byteoversea.net, it is routed to one or more of these sub-domains. The various

sub-domains are spread across the globe, including within China.

45. Defendants' taking of the Private Video Images is not disclosed in any of Defendants' privacy policies or other disclosure documentation. TikTok users are thus prevented from knowing that Defendants have taken their Private Video Images. No user consent exists.

3. The TikTok App Covertly Takes User/Device Identifiers.

46. Also unknown to TikTok users is that the seemingly innocuous TikTok app infiltrates their mobile devices and extracts a remarkably broad array of private and personally-identifiable data and content that Defendants use to track and profile TikTok users for the purpose of, among other things, targeting them with advertisements from which Defendants unjustly profit.

47. This unlawful secret taking of private and personally-identifiable data and content from TikTok users' mobile devices is contrary to American norms. The United States Supreme Court has recognized that, in contemporary society, cell phones are so ubiquitous and inextricably intertwined with the user's personal privacy that such devices have become "***almost a 'feature of human anatomy***.'" *Carpenter v. United States*, 138 S.Ct. 2206, 2218 (2018) (quoting *Riley v. California*, 573 U.S. 373, 385 (2014)). The United States Constitution thus provides a privacy right that protects individuals against unreasonable governmental searches of their physical movements through historical cell phone records in the possession of their service providers. *Carpenter*, 138 S.Ct. at 2218.

48. From each mobile device on which the TikTok app is installed, Defendants take a combination of, among other items, the following user identifiers and mobile device identifiers ("User/Device Identifiers"):

a. username, password, age/birthday, email address, and profile image;

b. user-generated content, including messages sent through the apps;

c. phone and social network contacts;

d. the mobile device's WiFi MAC address (*i.e.*, media access control address), which is the unique hardware number on the WiFi card adapter that tells the

internet who is connected to it;

e. the mobile device's International Mobile Equipment Identity ("IMEI") number, which is a unique number given to every mobile device that is used to route calls to one's phone, and that reflects information about the origin, model, and serial number of the mobile device;

f. the user's International Mobile Subscriber Identity ("IMSI") number, which is a unique number given to every subscriber to a mobile network;

g. the IP address (*i.e.*, Internet Protocol address), which is a numerical label assigned to each user mobile device connected to a computer network that uses the Internet Protocol for communication. IP addresses allow the location of literally billions of digital devices that are connected to the Internet to be pinpointed and differentiated from all other such devices;

h. the device ID, which is a unique, identifying number or group of numbers assigned to the user's individual mobile device that is separate from the hardware serial number;

i. the OS version, which is the operating system on the user's mobile device;

j. the mobile device brand and model/version;

k. the hardware serial number, which is the unique, identifying number or group of numbers assigned to the user's individual mobile device;

l. the Advertising ID, which is a unique ID for advertising that provides developers with a simple, standard system to monetize their apps;

m. mobile carrier information (*e.g.*, the name of the phone company);

n. network information, including the technology that the carrier uses;

o. browsing history;

p. cookies;

q. metadata; and

r. precise physical location, including based on SIM card, cell towers

and/or GPS.

49. Theft of physical and digital location tracking data is highly invasive of TikTok users' privacy rights. Two United States Senators observed that "[l]ocation data is among the most sensitive personal information that a user can share with a company … Today, modern smartphones can reveal location data beyond a mere street address. The technology is sophisticated enough to identify on which floor of a building the device is located."[40] Location data reveals ***private living patterns*** of TikTok users, including where they work, where they reside, where they go to school, and when they are at each of these locations. Location data, either standing alone or combined with other information, exposes deeply-private and personal information about TikTok users' ***health, religion, politics and intimate relationships***.

50. The TikTok app also invites users to sign in through Facebook, Google, and Twitter. What users do not know is that this "single sign-on" option gives Defendants access to TikTok users' private and personally-identifiable data and content stored on these ***other social media accounts***, including User/Device Identifiers such as the user's photos and friends/contacts information.

4. Defendants' Theft Of Private And Personally-Identifiable User Data And Content Begins Even Before Users Can Choose Whether To Sign Up With TikTok And Create An Account.

51. The TikTok app begins taking private and personally identifiable user data and content immediately upon the completion of the download process and before TikTok users even have the opportunity to sign-up and create an account. TikTok users therefore do not have an opportunity to learn about the existence of, much less consent to, any of Defendants' privacy policies or other disclosure documentation before the TikTok app begins mining their mobile devices for their data and content.

[40] https://www.law360.com/consumerprotection/articles/1221312/sens-prod-zuckerberg-why-keep-tracking-user-locations-.

5. Defendants' Theft Of Private And Personally-Identifiable Data And Content Continues Even After Users Close The TikTok App.

52. Even when TikTok users stop using the app and close it, Defendants continue to harvest private and personally-identifiable data and content from such users' mobile devices. There are no disclosures in any of Defendants' privacy policies or other disclosure documentation that such surreptitious taking of private and personally-identifiable user data and content occurs when the TikTok app is closed. TikTok users are thus prevented from knowing that Defendants have taken their private and personally-identifiable data and content while the TikTok app is closed. No user consent exists.

6. Defendants Carefully Conceal Their Misconduct.

53. At the same time that Defendants utilize the TikTok app to covertly tap into a massive array of private and personally-identifiable user data and content, they go to great lengths to hide their tracks. They do so by obfuscating the source code that would reveal the private and personally-identifiable user data and content actually taken from users' mobile devices.

7. Defendants' Privacy Policies And Terms Of Use Do Not Constitute Notice Of, Nor Consent To, TikTok User Data Theft, The Arbitration Provision Or The Class Action Waiver.

54. Defendants have adopted various privacy policies and terms of use for the TikTok app over the years. Certain privacy policies, revealed by investigation of counsel but not seen in the ordinary course by users, purport to disclose that the TikTok app takes certain (but not all) of the private and personally-identifiable user data and content above. Certain terms of use, revealed by investigation of counsel but not seen in the ordinary course by users, purport to require arbitration and class action waivers.

55. Because the TikTok app begins taking private and personally-identifiable user data and content – including User/Device Identifiers – immediately upon the completion of the download process, and before TikTok users are even presented with the

option of signing-up for and creating an account, TikTok users have no notice of, and cannot consent to, the privacy policies and terms of use prior to such theft. Moreover, because the TikTok app takes Private Videos and Private Video Images even if TikTok users have not signed up for an account, TikTok users who have not signed up for an account have no notice of, and cannot consent to, the privacy policies and terms of use prior to such theft.

56. Moreover, even at the point at which TikTok users have the option to sign-up and create an account, Defendants do not provide such users actual notice of privacy policies or terms of use. Nor do Defendants present TikTok users with conspicuously-located and designed hyperlinks to their privacy policies and terms of use, much less conspicuous warnings accompanying such hyperlinks. The TikTok app thus allows users to utilize it without ever placing them on actual or constructive notice of the privacy policies and terms of use. This lack of actual or constructive notice deprives TikTok users of the opportunity to accept or reject TikTok's privacy policies and terms of use, rendering such documents unenforceable. *See, e.g., Colgate v. Juul Labs, Inc.*, 402 F.Supp.3d 728 (N.D. Cal. 2019); *Arena v. Intuit Inc.*, 2020 WL 1189849 (N.D. Cal. 2020).

57. Additionally, certain privacy policies and terms of use are ambiguous as to what conduct they purport to cover. Such privacy policies and terms of use are also substantively and procedurally unconscionable. The ambiguities render meaningless the purported disclosures and requirements in the remainder of these documents, and the substantive and procedural unconscionability render such documents unenforceable.

58. Moreover, even if TikTok users in California had knowingly accepted the terms of use (which they did not), the purported waiver of the right to seek public injunctive relief in a court of law is unenforceable under California law. *See, e.g., McGill v. Citibank*, 2 Cal.5th 945 (2017); *Blair v. Rent-A-Center*, 928 F.3d 819 (9th Cir. 2019).

B. Defendants Come Under United States Government Scrutiny.

1. The United States Government Investigates Defendants' Stockpiling Of TikTok Users' Private And Personally-Identifiable Data And Content For The Chinese Government.

59. United States Senators Charles Schumer and Tom Cotton sent an October 2019 letter to the Acting Director of National Intelligence describing "national security" risks associated with the TikTok app. The Senators noted that there is evidence that Defendants may share private and personally-identifiable user data and content with the Chinese government:

> TikTok's terms of service and privacy policies describe how it collects data from its users and their devices, including user content and communications, IP address, location-related data, device identifiers, cookies, metadata, and other sensitive personal information. While the company has stated that TikTok does not operate in China and stores U.S. user data in the U.S., ByteDance is still required to adhere to the laws of China.
>
> Security experts have voiced concerns that China's vague patchwork of intelligence, national security, and cybersecurity laws compel Chinese companies to support and cooperate with intelligence work controlled by the Chinese Communist Party. … With over 110 million downloads in the U.S. alone, TikTok is a potential counterintelligence threat we cannot ignore. Given these concerns, we ask that the Intelligence Community conduct an assessment of the national security risks posed by TikTok … and brief Congress on these findings.[41]

60. The Committee on Foreign Investment in the United States ("CFIUS") is an inter-agency committee of the United States government that reviews the national security

[41] https://www.law360.com/articles/1213180/sens-want-tiktok-investigated-for-national-security-threats; https://www.cotton.senate.gov/?p=press_release&id=1239.

implications of foreign investments in United States companies or operations. Chaired by the United States Secretary of the Treasury, CFIUS includes representatives from 16 United States departments and agencies, including the Defense, State, Commerce and Homeland Security departments. CFIUS is reviewing Defendant Beijing ByteDance's acquisition of Defendants Musical.ly and Musical.ly, Inc.[42]

61. Additionally, the Senate Judiciary Subcommittee on Crime and Terrorism held a hearing in November 2019 that Defendant TikTok, Inc. declined to attend although it had been invited. The Chairman, Senator Josh Hawley, stated in opening remarks that: "TikTok should answer … to the millions of Americans who use their product with no idea of its risks."[43] Chairman Hawley also told reporters that: "The idea that TikTok is not sharing data, is not taking direction from Beijing, that just does not appear to be true."[44]

62. Indeed, the risk that Defendants send TikTok user data to the Chinese government is so great that the U.S. Army has banned the app on government-owned devices. That decision was based on concerns specific to Defendants and their close relationship to the Chinese government. The Army banned the TikTok app despite the fact that it had been using it for recruiting purposes until it realized the risk.[45] The U.S. Navy, Marines, Air Force and Coast Guard, as well as the Department of Defense and the Transportation Security Administration have likewise banned the TikTok app due to the risk that user data is being sent to China.[46]

---

[42] https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-views-about-censorship-often-were-overridden-by-chinese-bosses/.

[43] https://thehill.com/policy/technology/469114-tiktok-faces-lawmaker-anger-over-china-ties.

[44] https://thehill.com/policy/technology/469114-tiktok-faces-lawmaker-anger-over-china-ties.

[45] https://www.businessinsider.com/us-government-agencies-have-banned-tiktok-app-2020-2

[46] https://www.businessinsider.com/us-government-agencies-have-banned-tiktok-app-2020-2#1-the-navy-banned-tiktok-from-government-devices-1; https://www.engadget.com/2020-01-04-nearly-whole-us-military-bans-tiktok.html

2. Defendants Unpersuasively Deny They Transfer TikTok Users' Private And Personally-Identifiable Data And Content To The Chinese Government.

63. In July 2019, amid growing scrutiny, Defendant TikTok, Inc. retained consultants who opined that there is "no indication" that the Chinese government accessed TikTok users' data.[47] But the lead consultant admitted that the review and analysis was limited to a narrow and recent four-month period: "He added that in the analysis from July [2019] to October [2019], which included interviews with TikTok employees and a review of the app's underlying computer code, his team found no way TikTok could send data to China during those months."[48] And, the consultants did not address whether TikTok user data could be accessed from, as opposed to "sent to," China.

64. Defendant TikTok, Inc. also issued a public statement in which it represented: "First, let's talk about data privacy and security. We store all TikTok U.S. user data in the United States, with backup redundancy in Singapore. Our data centers are located entirely outside of China, and none of our data is subject to Chinese law."[49]

65. This public statement is carefully couched in the present tense and studiously avoids mention of past practices. In fact, the statement does not actually say that no private and personally-identifiable user data and content is transferred to China. Rather, it says that private and personally-identifiable user data and content is stored in the United States (but not necessarily exclusively in the United States) and that the current data centers are located outside China (but not whether these data centers transfer private and personally-identifiable user data to China or make it accessible there). Even Defendant TikTok, Inc.'s February 2019 Privacy Policy, which is not viewed by users in the ordinary course, states

---

[47] https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-views-about-censorship-often-were-overridden-by-chinese-bosses/.

[48] https://www.nytimes.com/2019/11/01/technology/tiktok-national-security-review.html.

[49] https://newsroom.tiktok.com/en-us/statement-on-tiktoks-content-moderation-and-data-security-practices.

that "[w]e may share your information with a parent, subsidiary, or other affiliate of our corporate group." Although this language is ambiguous, it apparently "means it would include China-based ByteDance."[50] Accordingly, Defendant TikTok, Inc.'s public statement (above) and its February 2019 Privacy Policy are, at best, highly misleading.

C. Transfers Of Private And Personally-Identifiable User Data And Content From TikTok Users To China Without Notice Or Consent.

1. The TikTok App Secretly Transfers Private And Personally-Identifiable User Data And Content To Servers In China.

66. *Affinity* published an article entitled "TikTok is Scamming People & Stealing Information." Quoting from a pre-2019 TikTok privacy policy, the article reports that "they store and process user data in United States of America, Singapore, Japan or to China."[51] The article also reports that Defendant TikTok, Inc. is "offering personal information to third parties and the Chinese government."[52]

67. *CNBC* published an article entitled "China's globally popular camera apps may open up user data to Beijing requests" in which it confirms that a TikTok privacy policy from 2018 acknowledged transmission of private and personally-identifiable user data and content to China: "TikTok's 2018 privacy policy said the company can transfer international users' data to China, according to archived versions of that web page."[53] Even Defendant TikTok, Inc.'s August 2018 Privacy Policy, which is not seen by users and which by its own terms does not even apply to United States users, states: "We will also share your information with any member or affiliate of our group, in China, for the purposes set out above, to assist in the improvement or optimisation of the Platform, …

---

[50] https://www.cnbc.com/2019/07/25/china-camera-apps-may-open-up-user-data-to-beijing-government-requests.html.

[51] http://culture.affinitymagazine.us/tik-tok-is-scamming-people-stealing-information/.

[52] http://culture.affinitymagazine.us/tik-tok-is-scamming-people-stealing-information/.

[53] https://www.cnbc.com/2019/07/25/china-camera-apps-may-open-up-user-data-to-beijing-government-requests.html.

increase user numbers, development, engineering and analysis of information or for our internal business purposes ….”

68. *Quartz* published an article by David Carroll entitled “Is TikTok a Chinese Cambridge Analytica data bomb waiting to explode?” Mr. Carroll is an associate professor at the Parsons School of Design in New York, and in 2017 he sued Cambridge Analytica in the United Kingdom. In his *Quartz* article, Mr. Carroll quoted from Defendant TikTok, Inc.’s August 2018 Privacy Policy that reveals that private and personally-identifiable user data and content is transferred to China.[54] Mr. Carroll further reported that, in emails between him and Defendant TikTok, Inc. in March and April 2019, Defendant TikTok, Inc. (i) confirmed that, at least prior to February 2019, U.S. TikTok user data may have been processed in China; and (ii) provided confusing answers about what happened after that, including that U.S. TikTok user data may have continued to be processed by systems operated by “one of our China registered entities,” and may exist there in some form, even where such user data is stored elsewhere.[55]

69. The *New York Times* has reported that a source “said the American government had evidence of the [TikTok] app sending data to China.”[56] That explains why the Defense Department, Navy, Army, Marines, Air Force, Coast Guard and Transportation Security Administration have taken the extraordinary step of prohibiting their members from using the TikTok app on any government-issued devices, and have advised that their children also remove the TikTok app from their devices.[57] United States Senators also have proposed a bill banning federal employees from using the TikTok app on government-issued phones because it “presents a major security risk.”[58]

---

[54] https://qz.com/1613020/tiktok-might-be-a-chinese-cambridge-analytica-scale-privacy-threat/.

[55] https://qz.com/1613020/tiktok-might-be-a-chinese-cambridge-analytica-scale-privacy-threat/.

[56] https://www.nytimes.com/2019/11/01/technology/tiktok-national-security-review.html.

[57] https://www.wsj.com/articles/u-s-military-bans-tiktok-over-ties-to-china-11578090613.

[58] https://www.reuters.com/article/us-usa-china-tiktok/us-senators-seek-to-ban-federal-employees-from-using-tiktok-on-their-phones-idUSKBN20Z1E4.

a. Evidence Of Post-February 2019 Transfers.

70. Even after Defendant TikTok, Inc. adopted its February 2019 Privacy Policy, the TikTok app secretly transferred private and personally-identifiable user data and content to China where, under Chinese law, it is subject to collection and use by the Chinese government. Specifically, Defendants used the TikTok app to transfer private and personally-identifiable user data and content to the following two servers in China as recently as April 2019: (i) bugly.qq.com and (ii) umeng.com.

71. Private and personally-identifiable TikTok user data and content transferred to bugly.qq.com as recently as April 2019 includes at least the following items: (i) the OS version; (ii) the mobile device model; (iii) the WiFi MAC address; (iv) the hardware serial number; (v) the device ID and (vi) the IP address. Private and personally-identifiable TikTok user data and content transferred to umeng.com as recently as April 2019 includes these same six items, plus at least the following item: (vii) the number of bytes users' mobile devices have uploaded and downloaded.

b. Evidence Of Pre-February 2019 Transfers.

72. The TikTok app transferred private and personally-identifiable TikTok user data and content to various servers in China prior to the February 2019 Privacy Policy, including to at least the following servers: (i) musemuse.cn; (ii) zhiliaoapp.com; (iii) mob.com; and (iv) umeng.com.

73. The private and personally-identifiable TikTok user data and content transferred to one or more of these four China-based servers includes biometrics and User/Device Identifiers. Additional private and personally-identifiable TikTok user data and content transferred to one or more of these four China-based servers includes: (i) a list of the other apps installed on users' mobile devices; and (ii) more specific location data. Such information reveals TikTok users' precise physical location, including possibly indoor locations within buildings, and TikTok users' apps that possibly reveal mental or physical health, religious views, political views, and sexual orientation.

2. Defendants' Privacy Policies Do Not Constitute Notice Of Or Consent To The Transfer Of Private And Personally-Identifiable TikTok User Data And Content To Servers In China.

74. TikTok users do not knowingly consent to Defendants' privacy policies because notice and warnings of the privacy policies are not adequately displayed, as discussed above. Additionally, many provisions of the privacy policies are ambiguous, providing inadequate notice of what private and personally-identifiable user data and content is taken and where it is being sent. Notably, even scholars with expertise in such matters, such as Mr. Carroll, cannot discern what is being taken and where it is going. Certainly, ordinary TikTok users cannot be expected to understand such baffling "disclosures." This ambiguity further renders the notice inadequate to establish informed user consent.

75. In addition to the above-stated deficiencies, privacy policy provisions stating that certain TikTok user data and content will be sent to servers in China is contradicted by Defendants' public assurances that no such transfers occur. Moreover, TikTok users whose data and content is sent before they even have an opportunity to sign-up and create an account do not actually or constructively receive notice, and therefore cannot be deemed to have assented to, such transfers to China.

3. The China-Based Tech Giants Also Possess TikTok Users' Private And Personally-Identifiable Data And Content While They Work Cooperatively With The Chinese Government.

76. The bugly.qq.com server is owned and operated by China-based tech giant Tencent Holdings Limited ("Tencent"), and the umeng.com server is owned and operated by another China-based tech giant Alibaba Holding Group Limited ("Alibaba"). Tencent and Alibaba thus possess TikTok users' private and personally-identifiable data and content. Such data transfers to Tencent and Alibaba servers were accomplished through Tencent and Alibaba source code that Defendants embedded within the TikTok app.

77. Also embedded within the TikTok app is source code from China-based tech

giant Baidu, Inc. ("Baidu") as well as source code from a China-based software development kit ("SDK") known as Igexin. The Igexin SDK is notorious for causing the removal of some 500 apps from the Google play store in 2017 after it was discovered that Igexin constituted a "secret backdoor" that allowed its operators "to install a range of spyware."[59] Specifically, Igexin "could update the app to include spyware at any time, with no warning. The most serious spyware installed on phones were packages that stole call histories, including the time a call was made, the number that placed the call, and whether the call went through. Other stolen data included GPS locations, lists of nearby Wi-Fi networks, and lists of installed apps."[60]

78. Baidu, Alibaba, and Tencent – popularly known by the acronym "BAT" – are "China's original tech titans"[61] and dominate the fields of artificial intelligence, social media, and the internet in China. The private and personally-identifiable TikTok user data and content they possess may well be used by the Chinese government in the future, if it has not already.

79. BAT routinely assist the Chinese government in the surveillance and control of its people through biometrics. "Biometric surveillance powered by artificial intelligence is categorically different than any surveillance we have seen before. It enables real-time location tracking and behavior policing of an entire population at a previously impossible scale."[62] The Chinese government is taking full advantage of China-based technology corporations like BAT to assist: "Beijing is embracing technologies like facial recognition and artificial intelligence to identify and track 1.4 billion people. It wants to assemble a vast and unprecedented national surveillance system, with crucial help from its thriving

---

[59] https://arstechnica.com/information-technology/2017/08/500-google-play-apps-with-100-million-downloads-had-spyware-backdoor/.

[60] https://arstechnica.com/information-technology/2017/08/500-google-play-apps-with-100-million-downloads-had-spyware-backdoor/.

[61] https://www.forbes.com/sites/rebeccafannin/2019/08/23/baidu-alibaba-tencent-clash-to-lead-chinas-tech-future-while-a-new-b-arises/#18cc42e414d0.

[62] https://www.buzzfeednews.com/article/evangreer/dont-regulate-facial-recognition-ban-it.

technology industry. … China has become the world's biggest market for security and surveillance technology, with analysts estimating the country will have almost 300 million cameras installed by 2020. Chinese buyers will snap up more than three-quarters of all servers designed to scan video footage for faces …."[63]

80. The Chinese government relies on China-based technology companies like BAT to assist in government investigations of criminal activity and political dissent, as well as surveillance activities: "The Chinese police 'request data from Alibaba for their own investigations, … tapping into the trove of information the tech giant collects through its e-commerce and financial payment networks. … Companies including Alibaba [], Tencent [], and Baidu [] are required to help China's government hunt down criminal suspects and silence political dissent. Their technology is also being used to create cities wired for surveillance. … Apple disclosed that more than 35,000 user accounts were affected by 24 Chinese law-enforcement requests in the first half of this year [2017], many in connection with fraud investigations. It said it provided information on about 90% of them. Chinese companies don't release any information on the number of requests from the government, the nature of the requests or the compliance rate.'"[64]

81. The Chinese government's use of BAT to sort and analyze information, including information gathered from smartphones, is also well documented: "Along with access to online data, China's government wants something else from tech companies – the cloud computing prowess to sort and analyze information. China wants to crunch data from surveillance cameras, smartphones, government databases and other sources to create so-called smart cities and safe cities. … Police now work with Alibaba to use surveillance footage and data processing to identify 'persons of interest' and keep them out, local police official Dai Jinming said at a recent conference sponsored by Alibaba. Tencent is working with police in the southern city of Guangzhou to build a cloud-based 'early-warning

[63] https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.

[64] https://www.wsj.com/articles/chinas-tech-giants-have-a-second-job-helping-the-government-see-everything-1512056284.

system' that can track and forecast the size and movement of crowds, according to a statement from the Guangzhou police bureau."[65]

82. The *Wall Street Journal* has reported on the significant patronage that BAT receive from the Chinese government, the growing number of tech entrepreneurs who have become members of the legislature under President Xi Jinping (including, for example, Tencent's Tony Ma), and BAT's pledges of loyalty to the Chinese government.[66] "'The government is always the boss and the tech firms are there to serve the goals of the Chinese government.'"[67]

83. Defendant Beijing ByteDance is emerging as a threat to BAT's exclusive status: "there's a new B in the BAT trio on the horizon: the world's highest-valued unicorn, ByteDance …."[68] Like BAT, Defendant Beijing ByteDance is subject to the same cybersecurity laws mandating cooperation with the Chinese government that are described in Senator Schumer and Senator Cotton's letter. Senator Hawley, according to the *Wall Street Journal*, described the resulting threat to TikTok users by stating: "all it takes is one knock on the door of their parent company [Defendant Beijing ByteDance], based in China, from a Communist Party official for that data [from Defendant TikTok, Inc.] to be transferred to the Chinese government's hands, whenever they need it."[69] In the same *Wall Street Journal* article, a former TikTok employee from the Los Angeles office stated that: "We're a Chinese company … We answer to China."[70]

---

[65] https://www.wsj.com/articles/chinas-tech-giants-have-a-second-job-helping-the-government-see-everything-1512056284.

[66] https://www.wsj.com/articles/the-godfathers-of-chinese-tech-get-an-offer-they-cant-refuse-1520510404.

[67] https://www.wsj.com/articles/the-godfathers-of-chinese-tech-get-an-offer-they-cant-refuse-1520510404.

[68] https://www.forbes.com/sites/rebeccafannin/2019/08/23/baidu-alibaba-tencent-clash-to-lead-chinas-tech-future-while-a-new-b-arises/#18cc42e414d0.

[69] https://www.wsj.com/articles/tiktok-looking-at-ways-to-shake-off-its-ties-to-china-11574073001.

[70] https://www.wsj.com/articles/tiktok-looking-at-ways-to-shake-off-its-ties-to-china-

84. A *Washington Post* opinion piece entitled "Could TikTok allow China to export repression?" describes the danger to TikTok users in the United States if Defendants provide such users' private and personally-identifiable data and content to the Chinese government: "TikTok's leaders protest that they store local information locally, so whatever data the company has on the behavioral patterns or personal attributes of some of the most vulnerable American citizens are not 'subject to Chinese law.' But it's reasonable to wonder whether TikTok might not comply with targeted intelligence requests from the repressive regime ruling over its parent company ByteDance. TikTok's younger users will be voting in the coming years; down the line, they may hold positions of power. A trove of their information is a valuable asset."[71]

85. The *Wall Street Journal*, in an article entitled "U.S. Orders Chinese Firm to Sell Dating App Grindr Over Blackmail Risk," also has reported on the dangers Americans face from the Chinese government's accumulation of their private and personally-identifiable data and content, including blackmail and other sinister scenarios: "U.S. national-security experts said Chinese government knowledge of an individual's usage of Grindr could be used in certain cases to blackmail U.S. officials and others with security clearances, such as defense contractors, and force them to provide information or other support to China. They have also envisioned more elaborate scenarios. For example, one could use Grindr's location data to discern that a certain user works at a telecommunications firm and pays regular visits to the same building in Northern Virginia that intelligence officials frequent. Chinese-intelligence officials could then determine that that individual is the telecommunications firm's intelligence liaison, and they would know both whom to target and how to threaten that person with potentially compromising information. … The risk has grown as the Chinese government acquires more large data sets through hacking and other means, allowing it to build databases with detailed profiles

11574073001.

[71] https://www.washingtonpost.com/opinions/global-opinions/could-tiktok-allow-china-to-export-repression/2019/11/02/1729f038-fa79-11e9-8906-ab6b60de9124_story.html.

of targets."[72]

VI. DEFENDANTS' THEFT OF TIKTOK USER BIOMETRICS.

A. The Illinois Biometric Information Privacy Act Regulates Face Geometry Scans, Voiceprints And Information Derived Therefrom.

86. In 2008, Illinois enacted the Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, *et seq.* This was due to the "very serious need [for] protections for the citizens of Illinois when it [comes to their] biometric information." Illinois House Transcript, 2008 Reg. Sess. No. 276. The Illinois Legislature recognized the importance of protecting the privacy of individuals' biometric data, finding that "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information." 740 ILCS 14/5(c). "For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse [and] is at heightened risk for identity theft …." *Id.*

87. BIPA thus focuses on "biometric identifiers" and "biometric information." Biometric identifiers consist of "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10. A "scan" under BIPA means to examine by observation or checking, or systematically in order to obtain data especially for display or storage. *In re Facebook Biometric Information Privacy Litigation*, 2018 WL 2197546, *3 (N.D. Cal. May 14, 2018). "Geometry" under BIPA is the relative arrangement of parts or elements. *Id*. Neither the term "scan" nor the term "geometry" require "actual or express measurements of spatial quantities like distance, depth, or angles." *Id*. Biometric information constitutes "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." 740 ILCS 14/10.

[72] https://www.wsj.com/articles/u-s-orders-chinese-company-to-sell-grindr-app-11553717942.

B. Defendants Unlawfully Collect, Use And Profit From TikTok User Biometrics, Face Geometry Scans, Voiceprints And Information Derived Therefrom.

88. Defendants' unlawful collection, possession, storage, dissemination, use and profiting from biometrics, face geometry scans and voiceprints of TikTok users, and the information derived therefrom, takes three forms.

89. ***First***, Defendants' BIPA and other biometrics-related violations are established by the functionality and code of the TikTok app itself. This functionality and code includes: (a) content recommendations based on TikTok users' race/ethnicity and age; (b) scans of face geometry to determine TikTok users' age; (c) censoring video content to remove people Defendants consider "ugly"; (d) the augmented reality feature that scans face geometry while processing users' videos; (e) code for deepfake videos; and (f) code for age, race/ethnicity and emotion recognition.

90. ***Second***, Defendants' BIPA and other biometrics-related violations are further established by their ongoing work in China, which includes: (a) the application of facial recognition technology[73] to TikTok users' videos by highly-trained engineers skilled in computer vision, convolutional neural network and machine learning; (b) patent applications for face, voice, age, race/ethnicity and emotion recognition technologies; and (c) the publicly-known functionality of Douyin that allows its users to perform facial recognition on faces selected by such users from other users' videos.

91. ***Third***, Defendants' BIPA and other biometrics-related violations are also established by Defendants' legal and political obligations to accumulate and share vast troves of data, including biometrics, in order to assist the Chinese government in meeting two crucial and intertwined state objectives: (a) world dominance in artificial intelligence;

[73] Facial recognition "is a technology capable of identifying or verifying a person from a digital image or a video frame from a video source. There are multiple methods in which facial recognition systems work, but in general, they work by comparing selected facial features from a given image with faces within a database." *See* https://en.wikipedia.org/wiki/Facial_recognition_system.

and (b) population surveillance and control.

1. Defendants' BIPA And Other Biometrics-Related Violations Are Evidenced By The TikTok App's Functionality And Code.

92. There are six specific categories of functions and code within the TikTok app that reveal BIPA violations: the race/ethnicity and age-based content recommendations; the scans to determine age; the removal of so-called "ugly" videos; the augmented reality feature; the deepfake video code; and the age, race/ethnicity and emotion recognition code.[74] These also evidence violations of the other statutory, constitutional and common law claims set forth herein.

93. That the TikTok app violates BIPA and other laws is highlighted by comments from a "Bytedance representative" who confessed to *The Verge* that "TikTok makes use of the company's AI technologies in various ways, from ***facial recognition for the filters*** through to the recommendation engine in the For You feed. … We build intelligent machines that are capable of understanding and analyzing text, images and ***videos*** using natural language processing and computer vision technology. This enables us to serve users with the content that they find most interesting ….'"[75]

94. Similarly, *Marketing Technology Insights* reported on Defendants' use of facial recognition technology in the TikTok app in violation of BIPA and other laws, stating that Defendant TikTok, Inc. and the TikTok app "deploy[] AI and ***Face Recognition technology*** to analyze user's interests and preferences through their interactions with the content, and display a personalized content feed to each user."[76]

a. Race/Ethnicity And Age Based Content Recommendations.

95. Marc Faddoul, a researcher at the University of California at Berkeley who

[74] This evidence also constitutes a basis for the other statutory, constitutional and common law causes of action herein.

[75] https://www.theverge.com/2018/11/30/18107732/bytedance-valuation-tiktok-china-startup (emphasis added).

[76] https://martechseries.com/mts-insights/staff-writers/pay-attention-to-tiktok-content/ (emphasis added).

studies artificial intelligence, conducted an experiment in or about February 2020 that revealed the TikTok app recommends content based in part on race/ethnicity and age information that it gleans from TikTok users' digital face images. *Buzzfeed* described his findings: "In the app, when a person follows a new account, they can click an arrow that then recommends other accounts to follow. Faddoul noticed that when he did this, the recommended accounts tended to look just like whoever he'd just followed — right down to ethnicity and hair color."[77]

96. *Recode* also reported on Faddoul's research in its article entitled "There's Something Strange About TikTok Recommendations":

> When artificial intelligence researcher Marc Faddoul joined TikTok a few days ago, he saw something concerning: When he followed a new account, the profiles recommended by TikTok seemed eerily, physically similar to the profile picture of the first account. Following a young-looking blond woman, for instance, yielded recommendations to follow more young-looking blond women. …
>
> Following black men led to recommendations to follow more black men. Following white men with beards produced recommendations for more white men with beards. Following elderly people spawned recommendations for other elderly people. And on and on. …
>
> Faddoul also told *Recode* that he believes it's more likely that TikTok is using something he calls automatic featurization. This type of recommendation algorithm could take "signals" from profile images to find profile pictures with similar attributes. These kinds of signals would be correlations between the pictures, which could correspond to anything from skin color to having a beard. The algorithm is simply looking for similarities in the photos or profiles. …

[77] https://www.buzzfeednews.com/article/laurenstrapagiel/tiktok-algorithim-racial-bias.

"What I suspect is happening is that TikTok is featurizing the profile picture," he says, "and using these features in the recommendation engine."[78]

b. Face Scans To Determine Age.

97. Defendants also scan face images taken from TikTok user videos in order to determine TikTok users' age. The *Wall Street Journal* has reported that "TikTok has built an artificial intelligence tool that scans faces in videos to estimate users' ages."[79] Both Faddoul's research and this *Wall Street Journal* article are consistent with evidence of Defendants' work in China on TikTok user videos as well as their patent applications in China for face, voice, age, race/ethnicity and emotion recognition technologies (below).

c. Removal Of Videos Of So-Called "Ugly" People.

98. Public reporting indicates that "the makers of TikTok … instructed moderators to suppress posts created by users deemed too ugly …. Today, *The Intercept* and *The Intercept Brasil* are publishing two internal TikTok moderation documents …. One … describes algorithmic punishments for unattractive and impoverished users. The documents appear to have been originally drafted in Chinese and later — at times awkwardly — translated into English for use in TikTok's global offices."[80] Defendant TikTok, Inc. uses artificial intelligence technology in its Culver City office to review and flag user content. Given the presence of this AI technology and the sheer volume of TikTok user videos that are reviewed for "ugliness," it is apparent that Defendant TikTok, Inc. is using facial recognition technology to identify and remove such users' videos.

d. Augmented Reality Features.

99. The TikTok app uses an advanced video editor and camera face filters. Employing this technology, TikTok users edit their videos to, among other things, morph their face into another face; change the size, shape, height and width of their face; change

---

[78] https://www.vox.com/recode/2020/2/25/21152585/tiktok-recommendations-profile-look-alike.

[79] https://www.wsj.com/articles/tiktok-wants-to-grow-up-but-finds-it-tough-to-keep-kids-out-11581858006.

[80] https://theintercept.com/2020/03/16/tiktok-app-moderators-users-discrimination/.

particular features of their face (*e.g.*, eyes, ears, nose, lips, mouth, cheeks), including the size and shape of such facial features; and so on. Users thereby create videos in which their faces and specific facial features take on cartoonish dimensions and appearances, and in which they can appear older, etc.

100. This functionality is a form of augmented reality ("AR").[81] To perform AR, the TikTok app examines, detects and localizes the face and the arrangement of its various parts (*e.g.*, the eyes, ears, nose, lips, mouth, cheeks) relative to the other parts, and then also tracks the face and its various parts (and their relative arrangement) while in motion.

101. The following relevant code is located within the TikTok app: "FaceDetectManager"; "faceDetectMaxTime"; "faceDetectMinTime"; "Requirement_Face_3D_Detect"; "Requirement_Face_Detect"; "Requirement_Face_Track"; "face_track.model"; "maxScanTime"; "minScanTime"; and "faceID". Additional code for pitch, yaw and roll – "the three dimensions of movement when an object moves through a medium"[82] – is within the TikTok app as well.

102. This functionality and code reveal Defendants' use of face geometry scans on TikTok users. While it is currently unclear whether Defendants upload such face geometry scans from TikTok users' mobile devices, in addition to performing separate face geometry scans at the server level, this functionality and code demonstrate Defendants' technological ability and willingness to perform such scans on TikTok users.

---

[81] AR "is an interactive experience of a real-world environment where the objects that reside in the real world are enhanced by computer-generated perceptual information …. AR can be defined as a system that fulfills three basic features: a combination of real and virtual worlds, real-time interaction, and accurate 3D registration of virtual and real objects. … This experience is seamlessly interwoven with the physical world such that it is perceived as an immersive aspect of the real environment. In this way, augmented reality alters one's ongoing perception of a real-world environment …. With the help of advanced AR technologies (e.g. adding computer vision, incorporating AR cameras into smartphone applications and object recognition) the information about the surrounding real world of the user becomes interactive and digitally manipulated." *See* https://en.wikipedia.org/wiki/Augmented_reality.

[82] https://simple.wikipedia.org/wiki/Pitch,_yaw,_and_roll.

e. Code For Deepfake Videos.

103. There is code within the TikTok app, as well as within Douyin, for performing facial recognition. *TechCrunch* reported that there is "Face Swap" code within the TikTok app for "life-like deepfakes technology." It "asks users to take a multi-angle biometric scan of their face, then choose from a selection of videos they want to add their face to and share."[83] Defendants admitted that such code is present in the TikTok app, but denied its use. A TikTok spokesperson "insisted that 'after checking with the teams I can confirm this is definitely not a function in TikTok ….' They later told *TechCrunch* that 'the inactive code fragments are being removed to eliminate any confusion,' which implicitly confirms that Face Swap code was found in TikTok."[84]

104. That the "Face Swap" code is present in the TikTok app demonstrates Defendants' technological capacity and intent to perform facial recognition on TikTok users. Further, the "Face Swap" code further confirms the direct involvement of Defendant Beijing ByteDance in the TikTok app, because there would otherwise be no way for the TikTok app to include facial recognition code that Defendants TikTok, Inc. and ByteDance, Inc. have denied was ever used in the United States.

f. Code For Age, Race/Ethnicity And Emotion Recognition.

105. There is additional code within the TikTok app designed to recognize users' age, race/ethnicity and emotions. The code separates race/ethnicity into at least four categories: "Blac" [*sic.*]; "Indian"; "White"; and "Yellow." The code also distinguishes between at least seven different ranges of emotion: "Angry"; "Disgust"; "Fear"; "Happy"; "Neutral"; "Sad"; and "Surprise."

106. To place TikTok users within one of these categories, the TikTok app would have to use face geometry scans and/or voiceprints. It is currently unclear whether this code is active at the mobile device level and, if so, whether Defendants upload any such

---

[83] https://techcrunch.com/2020/01/03/tiktok-deepfakes-face-swap/.

[84] https://techcrunch.com/2020/01/03/tiktok-deepfakes-face-swap/.

face geometry scans and voiceprints from TikTok users' mobile devices. Nonetheless, the age, race/ethnicity and emotion recognition code within the TikTok app is consistent with Faddoul's research (above) and also directly correlates to Defendants' China-based work on TikTok user videos and patent applications (below).

2. Defendants' BIPA And Other Biometrics-Related Violations Are Further Evidenced By Defendants' China-Based Operations.

107. Defendants' BIPA violations are further established by their ongoing work in China, which includes: (a) the application of facial recognition technology to TikTok users' videos by highly-trained engineers skilled in computer vision, convolutional neural network and machine learning; (b) patent applications for face, voice, age, race/ethnicity and emotion recognition technologies; and (c) the Douyin app's functionality that allows its users to perform facial recognition on faces selected by such users from other users' videos. These factors also evidence violations of the other statutory, constitutional and common law claims set forth herein.

a. Defendants' China-Based Team Of Highly-Skilled Computer Vision, Convolutional Neural Network, And Machine Learning Engineers.

108. Defendants' artificial intelligence work within China, which is closely tied to its United States operations, is among the most sophisticated in the world. "ByteDance has received accolades for being a top AI innovator from CBInsight who recognized the company on its 2018 AI 100 List as well as from Fast Company, who placed it on its most innovative companies list. In 2016, it founded its AI Lab, a research division led by Wei-Ying Ma, formerly of Microsoft Research Asia. The Lab's primary focus has been on developing innovative technologies to enhance ByteDance's content platforms."[85]

109. Defendants have a team of engineers in cutting-edge fields such as computer

[85] https://www.forbes.com/sites/bernardmarr/2018/12/05/ai-in-china-how-buzzfeed-rival-bytedance-uses-machine-learning-to-revolutionize-the-news/#6579bada40db.

vision,[86] convolutional neural network ("CNN"),[87] and machine learning,[88] all of which are foundational to the face geometry scans and voiceprints that Defendants conduct on and/or derive from the Private Videos and the posted videos of TikTok users.

110. Defendants' China-based engineering team includes, among others: (i) a research scientist focused on facial recognition, object detection, computer vision and machine learning who has worked for Defendants since 2018; (ii) a computer vision and image processing algorithm engineer who has worked for Defendants since 2017; (iii) a computer vision algorithm engineer who has worked for Defendants since 2019; (iv) a machine learning and neural network engineer who has worked for Defendants since 2017; (v) an algorithm engineer who focuses on video retrieval and who has worked for Defendants since 2018; and (vi) an algorithm engineer who has worked for Defendants

---

[86] Computer vision "is an interdisciplinary scientific field that deals with how computers can gain high-level understanding from digital images or videos. … Computer vision tasks include methods for acquiring, processing, analyzing and understanding digital images …. The classical problem in computer vision, image processing, and machine vision is that of determining whether or not the image data contains some specific object, feature, or activity. … • Object recognition (also called object classification) – one or several pre-specified or learned objects or object classes can be recognized, usually together with their 2D positions in the image or 3D poses in the scene. … • Identification – an individual instance of an object is recognized. Examples include identification of a specific person's face or fingerprint …. • Detection – the image data are scanned for a specific condition. … Currently, the best algorithms for such tasks are based on convolutional neural networks. … Several specialized tasks based on recognition exist, such as: • Content-based image retrieval – finding all images in a larger set of images which have a specific content. … • Facial recognition." *See* https://en.wikipedia.org/wiki/Computer_vision#Recognition.

[87] CNN "is a class of deep neural networks, most commonly applied to analyzing visual imagery. … They have applications in image and video recognition, recommender systems, [and] image classification …. CNNs use relatively little pre-processing compared to other image classification algorithms. This means that the network learns the filters that in traditional algorithms were hand-engineered. This independence from prior knowledge and human effort in feature design is a major advantage." *See* https://en.wikipedia.org/wiki/Convolutional_neural_network#Image_recognition.

[88] Machine learning "is the study of computer algorithms that improve automatically through experience. It is seen as a subset of artificial intelligence. Machine learning algorithms build a mathematical model based on sample data, known as "training data", in order to make predictions or decisions without being explicitly programmed to do so. Machine learning algorithms are used in a wide variety of applications, such as … computer vision, where it is difficult or infeasible to develop conventional algorithms to perform the needed tasks." *See* https://en.wikipedia.org/wiki/Machine_learning.

since 2017.

b. Facial Recognition Technology Applied To TikTok Videos.

111. Wei-Ying Ma is a ByteDance Vice President in Beijing and has led the AI Lab since 2017. He is known for having developed a highly respected image retrieval system called NeTra, which is a tool for navigating very large image databases. Ma recently delivered a keynote speech at a Taipei Web Conference in which he acknowledged that Defendants use facial recognition technology and face geometry scans on their enormous and ever-growing database of face images from user videos. During his speech, Ma used visual representations that show facial recognition and face geometry scans being performed on specific regions of face images. Chinese language text accompanying the face images indicate the type of facial expression and the age of the individuals represented by the face images. English language notes to the side of the face images refer to "emotion analysis," "object detection and tracking," and "content-based recommendation." Ma made the following representations during his speech while these face images, accompanied by the aforementioned Chinese language and English language statements, were visually presented on the screen:

> We are actually receiving a huge number of video created by users every day, so it's at the hundreds of millions of video per day. Imagine the amount of computation and also video understanding we need to do here. And here just to give you a glimpse of all kinds of video understanding tasks we need to run, and let me show you for example, you just saw that video, and for video like that we actually do all kind of analysis. We need to automatically classify and also do a lot tagging and understand the structure inside the video and also run copyright infringement detecting and duplicate detection and also object detection and tracking. So based on this video, we convert this video into a structural representation, and here just to give you one of the

examples.[89]

112. Defendants' team of engineers in China also includes a computer vision and machine learning engineer who has worked for Defendants since 2018. His job responsibilities have included face/body detection and face attribute recognition, ***including specifically on TikTok users' videos***.

113. Within China, Defendant Beijing ByteDance makes no secret of its processing and analysis of users' videos from around the world. *TechNode* reported that one of its vice presidents publicly told a gathering that "ByteDance" required more chips to continue uploading, processing and analyzing its vast database of videos accumulated from around the world. This vice president stated that "'Bytedance has the largest number of users in ***the world*** whose ***videos*** need to be analyzed and processed and uploaded, and we are purchasing a large number of chips.'"[90]

114. Defendants' wealth of video recordings from TikTok users is critical to Defendants' success in making the TikTok app one of the most popular in the world: "The [TikTok] app heavily utilizes AI that is trained on the vast quantity of ***video footage*** to understand the preferences of users, while also using machine learning to make creating, editing, and promoting the ***videos*** as easy as possible."[91]

115. Indeed, "***all of ByteDance's products*** use artificial intelligence and machine learning to deliver content that users want. The company's intelligent machines use computer vision and natural language processing technology to understand and analyze written content, images and ***videos***. Then, based upon what the machines know about each user, they deliver the content it believes each user would want. As a user interacts with the content by taps, swipes, time spent with each article, comments and more, large-scale machine learning and deep learning algorithms continue to learn about a user's preferences

[89] https://www.youtube.com/watch?v=2D29f4-J2mw (at 18:18 – 19:17).

[90] https://technode.com/2018/04/24/bytedance-jinri-toutiao-ai-chips/ (emphasis added).

[91] https://dzone.com/articles/the-data-thats-driving-chinas-hidden-champions (emphasis added).

to refine its content delivery for the future. The end result is a high-quality content feed based upon each user's preferences and interests. As more content is accumulated by the system, the better the algorithms get to enhance the content experience."[92]

c. Face, Age, Race/Ethnicity And Emotion Recognition Patent Applications.

116. One of Defendants' engineers in China stands out for his inventions that form the basis of numerous patent applications filed by Defendants' sister company Beijing ByteDance Network Technology Co., Ltd. The underlying technology in these patent applications involves age, race and emotion detection through face images, including those derived from videos. The specific patent applications include, among others, the following:

a. Facial image identifying method.[93]

b. Use of face images and a facial recognition model to determine ethnic information, to then determine race, to ultimately determine age.[94]

c. Use of face and body images, and a facial recognition model, to determine age.[95]

d. Use of image data sets and audio data sets to determine age.[96]

e. Use of face images extracted from videos to determine age.[97]

f. Use of face images extracted from videos to determine age.[98]

g. Human facial expression recognition method.[99]

---

[92] https://www.forbes.com/sites/bernardmarr/2018/12/05/ai-in-china-how-buzzfeed-rival-bytedance-uses-machine-learning-to-revolutionize-the-news/#6579bada40db (emphasis added).

[93] Publication No. WO2020037963A1.

[94] Publication No. CN110046571A.

[95] Publication No. CN109993150A.

[96] Publication No. CN110321863A.

[97] Publication No. CN110163170A.

[98] Publication No. CN110188660A.

h. Use of face images extracted from videos to determine emotions based on expression recognition.[100]

i. Use of face images extracted from video segments to identify a face characteristic by parsing the face image.[101]

117. This same engineer was one of the inventors involved in two earlier patent applications filed by a Chinese university that concern face attribute recognition[102] and a face verification method that determines whether faces in two images are the same or distinct.[103]

118. "TikTok's owner, Beijing-based ByteDance, is a hit app factory that has spent the last decade learning how to use artificial intelligence, machine learning, and ***facial recognition*** to figure out what people like and serve them endless streams of entertainment tailored to their interests and ***emotions***. Its apps are used by billions of people, including 1.45 billion global downloads for TikTok alone. The company has years of data informing it on ***how people think, feel and act***, making it an expert on ***what makes people tick and how to persuade them*** to watch, share or like certain content."[104]

d. Voiceprint Patent Applications.

119. Beijing ByteDance Network Technology Co., Ltd. filed additional patent applications for a method for voice extraction involving voiceprints,[105] a voice recognition method,[106] and an age recognition method based on audio.[107] This is consistent with

---

[99] Publication No. CN110097004A.

[100] Publication No. CN110175565A.

[101] Publication No. CN110163171A.

[102] Publication No. CN106203395B.

[103] Publication No. CN106203533B.

[104] https://www.bloomberg.com/news/newsletters/2019-10-29/worries-that-tiktok-is-a-threat-to-national-security-have-merit (emphasis added).

[105] Publication No. CN110503961A.

[106] Publication No. WO2019214628A1.

reporting that Defendant Beijing ByteDance "uses various AI technologies in its services [including] ***voice recognition*** …."[108] In fact, during Wei-Ying Ma's recent keynote speech at a Taipei Web Conference (above), he discussed the use of audio to identify speakers and he published a slide during his speech entitled "Speaker Identification" that stated: "Detect identity, age, gender of speakers."[109]

e. The Douyin App's Facial Recognition Function.

120. The Douyin app provides its users with an "in-video" search tool that uses facial recognition technology. Users of Douyin can press the "Search" button while a video is playing, drag a rectangle around the target face in the video, and cause the Douyin app to perform a search (based on the face in question) for other videos in which the targeted person appears.[110] This subjects anyone using the Douyin app to "behind-the-scenes ***facial recognition*** analysis."[111] While U.S. TikTok users cannot access this feature, there is evidence that they are subject to the same behind-the-scenes facial recognition analysis, as discussed herein.

3. Defendants' BIPA And Other Biometrics-Related Violations Are Also Evidenced By Their Obligation To Accumulate And Share Data, Including Biometrics, With The Chinese Government.

121. Defendants' BIPA violations are further established by Defendants' legal and political obligations to accumulate and share data, including biometrics, in order to assist the Chinese government in meeting two crucial and intertwined state objectives: (a) world dominance in artificial intelligence; and (b) population surveillance and control.[112]

---

[107] Publication No. CN110335626A.

[108] https://medium.com/syncedreview/intel-and-bytedance-partner-on-ai-lab-b678036cbda4 (emphasis added).

[109] https://www.youtube.com/watch?v=2D29f4-J2mw (at 30:04).

[110] https://radiichina.com/tiktok-new-video-search-function-is-from-the-future/.

[111] https://futurism.com/the-byte/tiktok-facial-recognition (emphasis added).

[112] This evidence also constitutes a basis for the other statutory, constitutional and common law

a. The Chinese Government's Plan To Become The World Leader In Artificial Intelligence.

122. In 2017, the Chinese government released its Next Generation Artificial Intelligence Development Plan, in which it set 2030 as the temporal goal for becoming the world leader in artificial intelligence. To ensure achievement of its artificial intelligence goal, the Chinese government selected the five leading technology companies as "national champions" and assigned them particular areas of research and development within the artificial intelligence field. In exchange, these companies receive government support, including access to finance, preferential contract bidding and sometimes market share protection. The list of "national champions" has grown to at least 15 in recent years.[113]

123. The United States government has taken notice. Last November, Congress's National Security Commission on Artificial Intelligence, chaired by former Google CEO Eric Schmidt, published an interim report warning that China was outpacing the United States in artificial intelligence spending.[114]

b. The Chinese Government's Program Of Population Surveillance And Control.

124. The Chinese government's monitoring of and control over its own population are well known. Most notable is its pervasive use of artificial intelligence-enabled cameras to conduct video surveillance of its population.[115] As the *South China Morning Post* reported: "China's goal of becoming a global leader in artificial intelligence (AI) is nowhere more manifested than in how facial recognition technology has become a part of daily life in the world's second-largest economy. Facial recognition systems, which are biometric computer applications that automatically identify an individual from a database of digital images, are now being used extensively in areas such as public security,

causes of action herein.

[113] https://fortune.com/longform/tiktok-app-artificial-intelligence-addictive-bytedance-china/.

[114] https://fortune.com/longform/tiktok-app-artificial-intelligence-addictive-bytedance-china/.

[115] https://fortune.com/longform/tiktok-app-artificial-intelligence-addictive-bytedance-china/.

financial services, transport and retail across the country."[116] In fact, the Chinese government employs a variety of biometrics for population surveillance and control: "In addition to voice recognition, there are facial and pupil recognition, gathering of DNA samples—building the world's largest DNA database—and fingerprint scans."[117]

c. Data Accumulation, Including Biometrics, Through China-Based Technology Companies Is A Critical Part Of Achieving The Chinese Government's Twin Goals.

125. Artificial intelligence algorithms feed on data to learn and improve – thus, the more data the better the development of the algorithms driving the advance of the artificial intelligence.[118] With better artificial intelligence comes more effective population surveillance and control.

126. To advance these interrelated goals, the Chinese government has worked hand in glove with China-based technology companies to accumulate and share data. For example, the China-based company Megvii, a leader in computer vision, has the world's largest open source database (Face++) for training other facial recognition algorithms. It has reportedly used government data banks to help compile this training program.[119] As another example, the Chinese government partnered with the China-based technology firm d-Ear Technologies to build a database of voiceprints for voice recognition purposes.[120]

127. "Private [China-based] corporations and the [Chinese] Communist Party's security apparatus have grown together, discovering how the same data sets can both cater to consumers and help commissars calibrate repression. … Many [China-based] tech firms

---

[116] https://www.scmp.com/tech/start-ups/article/2133234/meet-five-chinese-start-ups-pushing-facial-recognition-technology.

[117] https://vlifestyle.org/codec-news/?l=business/content-2254742-china-gathers-people-s-voices-new-identification-technology-drawing-concerns.

[118] https://fortune.com/longform/tiktok-app-artificial-intelligence-addictive-bytedance-china/.

[119] https://fortune.com/longform/tiktok-app-artificial-intelligence-addictive-bytedance-china/.

[120] https://vlifestyle.org/codec-news/?l=business/content-2254742-china-gathers-people-s-voices-new-identification-technology-drawing-concerns.

make a point of hiring the relatives of high party officials, and a vast state database of headshots might be shared with a private firm to train new facial recognition software, while the firm's trove of real-time user data might be offered to police, for a panoramic view of potential 'troublemakers.'"[121]

128. Such data accumulation is not confined to China's borders. For example, the Chinese government is compiling a tremendous storehouse of private and personally-identifiable data on ordinary Americans. Recently, Chinese government-sponsored hackers stole data belonging to approximately 500 million Marriott International guests. "[M]achine learning is yielding uses for large data sets that humans alone could not imagine – or even understand – given that machine learning can generate correlations among data that the machine itself can't explain. … Beijing's plan may be simply to vacuum up as much data like this as possible and *then* see what today's machine learning—or, better yet, tomorrow's machine learning—can do with it."[122]

129. The lengths to which the Chinese government will go to obtain such data about ordinary Americans is further evidenced by other large-scale hacking schemes, including one involving 145 million Americans whose data was held by Equifax,[123] and another involving 78 million Americans whose data was held by Anthem.[124] "The United States assessed that China was building a vast database of who worked with whom in national security jobs, where they traveled and what their health histories were, according to American officials. Over time, China can use the data sets to improve its artificial intelligence capabilities to the point where it can predict which Americans will be primed for future grooming and recruitment …."[125] "The hacks, security researchers said, were an

---

[121] https://www.nytimes.com/interactive/2019/05/02/opinion/will-china-export-its-illiberal-innovation.html.

[122] https://www.justsecurity.org/62187/weapons-mass-consumerism-china-personal-information/.

[123] https://www.nytimes.com/2020/02/10/us/politics/equifax-hack-china.html.

[124] https://www.nytimes.com/2019/05/09/technology/anthem-hack-indicted-breach.html.

[125] https://www.nytimes.com/2020/02/10/us/politics/equifax-hack-china.html.

extension of China's evolving algorithmic surveillance system, which has greatly expanded over the past few years."[126]

130. The Chinese government's goal of obtaining private and personally-identifiable data (including biometrics) of ordinary citizens throughout the world is also evidenced by the deal struck by China-based CloudWalk Technology in Africa. CloudWalk, with the Chinese government's blessing, entered into a strategic partnership agreement with Zimbabwe to begin a large-scale facial recognition program. With access to a database containing millions of Zimbabwean faces, CloudWalk and the Chinese government intend to train their algorithms in order to further improve their facial recognition capabilities. "With the largest surveillance system already in place, ***China is also building one of the world's most comprehensive facial recognition databases***. Rolling out the technology in a majority black population will allow CloudWalk to more clearly identify other ethnicities, getting ahead of US and European developers."[127]

d. Defendants Are Obligated By Chinese Law And Politics To Accumulate And Secretly Share Their Data, Including Biometrics, With The Chinese Government.

131. Given the Chinese government's illegal extraction of massive quantities of private and personally-identifiable data (including biometrics) from hundreds of millions of ordinary Americans and others, there is no reason to believe that the Chinese government has refrained from extracting the same type of U.S. TikTok user data from Defendants. In fact, to access that data, there is no need to hack major U.S. corporations or the China-based technology companies, like Defendants, that have surreptitiously amassed such information on their own. That is because such China-based companies are ***required by law*** to ***secretly*** provide that data to the government upon demand:

The message contained in each of China's state security laws passed since

[126] https://www.nytimes.com/2019/05/09/technology/anthem-hack-indicted-breach.html.

[127] https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity/ (emphasis added).

> the beginning of 2014 is clear: everyone is responsible for the party-state's security. According to the CCP's definition of state security, the Party's political leadership is central. … And the party expects Chinese people and citizens to assist in collecting intelligence. The Intelligence Law states 'any organization and citizen shall, in accordance with the law, support, provide assistance, and cooperate in national intelligence work, and guard the secrecy of any national intelligence work that they are aware of…' Not only is everyone required to participate in intelligence work when asked, but that participation must be kept secret.[128]

132. Consequently, Defendants must "support, provide assistance and cooperate" by accumulating TikTok user data, including biometrics such as face geometry scans, voiceprints and information derived therefrom, and then share such data with the Chinese government. In an article entitled "Take China's TikTok App Security Threat Seriously," *Bloomberg* reported that many "Hong Kong protesters say that regardless of whether TikTok is censoring content or not, they fear posting on a social media site owned by ByteDance, a Beijing company that must hand over user information to Chinese authorities if asked, just like all its compatriots."[129]

133. In fact, Defendants in this action – including even the two based in the United States (Defendants TikTok, Inc. and ByteDance, Inc.) – have objected to Plaintiff Misty Hong's requests for the production of relevant documents in this lawsuit "to the extent they seek state secrets or any other information that cannot be disclosed without violating Chinese law, including the People's Republic of China on Guarding State Secrets and/or Civil Procedure Law of the People's Republic of China ("State Secrets")." Defendants apparently interposed this "State Secrets" objection in order to comply with

---

[128] https://capx.co/britain-must-avoid-being-sucked-into-huaweis-moral-vacuum/. *See also* https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense.

[129] https://www.bloomberg.com/news/newsletters/2019-10-29/worries-that-tiktok-is-a-threat-to-national-security-have-merit.

China's Intelligence Law requirement that "[n]ot only is everyone required to participate in intelligence work when asked, but that participation must be kept secret."[130] This "State Secrets" objection flatly contradicts Defendant TikTok, Inc.'s misleading public statement that "none of our data is subject to Chinese law."[131]

134. Defendant Beijing ByteDance has a particularly strong incentive to cooperate with the Chinese government. In 2018, China's State Administration of Radio and Television, an arm of the Chinese Communist Party, ordered Defendant Beijing ByteDance to shut down one of its apps due to "vulgar" content. That prompted the CEO of Defendant Beijing ByteDance to publicly apologize. His re-dedication to the Chinese Communist Party resulted in his being named one of the "100 outstanding private entrepreneurs" who were "chosen for being 'emblematic of the country's private economic development', while also being people who 'resolutely uphold the Party's leadership ....'"[132]

135. In a further show of allegiance to the Chinese government, Defendant Beijing ByteDance actively supports and participates in the spreading of Communist Party propaganda. It signed a strategic cooperation agreement with the Ministry of Public Security's Press and Publicity Bureau to promote the credibility of the police department, including within an area of China known for severe repression, demolition of mosques, and wide-spread detention centers for ethnic minorities. Under that agreement, "all levels and divisions of police units from the Ministry of Public Security to county-level traffic police would have their own Douyin account to disseminate propaganda. The agreement also reportedly says ByteDance would increase its offline cooperation with the police department …."[133]

---

[130] https://capx.co/britain-must-avoid-being-sucked-into-huaweis-moral-vacuum/.

[131] https://newsroom.tiktok.com/en-us/statement-on-tiktoks-content-moderation-and-data-security-practices.

[132] https://chinatechmap.aspi.org.au/#/company/bytedance.

[133] https://chinatechmap.aspi.org.au/#/company/bytedance. *See also*

136. Combined with evidence of the TikTok's app's functionality and code, the application of facial recognition technology to TikTok user videos, the patent applications for facial, voice, age, race/ethnicity and emotion recognition technologies, and the Douyin app's facial recognition feature, Defendants' legal obligations and political ties to the Chinese government make clear their large-scale BIPA and other biometrics violations.

VII. DEFENDANTS UNJUSTLY PROFIT WHILE PLAINTIFFS, THE CLASS AND THE TWO SUBCLASSES SUFFER HARM.

137. Defendants use the User/Device Identifiers, the biometric identifiers and information, and the Private Videos and Private Video Images to create a dossier of private and personally-identifiable data and content for each TikTok user. These are living files that are supplemented over time with additional private and personally-identifiable user data and content, and utilized in the past, the present and the future for economic and financial gain.

138. Defendants' unlawful possession and control over these ever-expanding dossiers make tracking and profiling TikTok users, and targeting them with advertising, much more efficient, effective and lucrative. These living dossiers of private and personally-identifiable data and content are used to analyze TikTok users' income, consumption habits, and preferences. Such information provides guidance as to what methods of advertising will be most effective on particular TikTok users, what products – including Defendants' own products – will be most attractive to particular TikTok users, and how much to spend on particular ads. Defendants unjustly have earned and continue to earn substantial profits and revenues from such targeted advertising and from generating increased demand for and use of Defendants' other products.

139. Defendants also unlawfully leverage these living dossiers of private and personally-identifiable TikTok user data and content to improve their artificial intelligence technologies and file patent applications, thereby unjustly increasing their past, present and

https://www.washingtonpost.com/world/tiktoks-owner-is-helping-chinas-campaign-of-repression-in-xinjiang-report-finds/2019/11/28/98e8d9e4-119f-11ea-bf62-eadd5d11f559_story.html.

future profits and revenues – and their market value.

140. Meanwhile, Plaintiffs, the Class and the Subclasses have incurred, and continue to incur, harm as a result of the invasion of privacy stemming from Defendants' covert theft of their private and personally-identifiable data and content – including their User/Device Identifiers, biometric identifiers and information, and Private Videos and Private Video Images. Plaintiffs, the Class and the Subclasses also have suffered and continue to suffer harm in the form of diminution of the value of their private and personally-identifiable data and content as a result of Defendants' surreptitious and unlawful activities. Moreover, Plaintiffs, the Class and the Subclasses have suffered and continue to suffer injuries to their mobile devices. The battery, memory, CPU and bandwidth of such devices have been compromised, and as a result the functioning of such devices has been impaired and slowed, due to Defendants' clandestine and unlawful activities. Finally, Plaintiffs, the Class and the two Subclasses have incurred additional data usage and electricity costs that they would not have incurred but for Defendants' covert and unlawful actions.

VIII. FRAUDULENT CONCEALMENT AND TOLLING.

141. The applicable statutes of limitations are tolled as a result of Defendants' knowing and active concealment of their unlawful conduct alleged above – through, among other things, their obfuscation of the source code, misleading public statements, and hidden and ambiguous privacy policies and terms of use. Plaintiffs, the Class and the two Subclasses were ignorant of the information essential to pursue their claims, without any fault or lack of diligence on their own part.

142. Also, at the time the action was filed, Defendants were under a duty to disclose the true character, quality, and nature of their activities to Plaintiffs, the Class and the two Subclasses. Defendants are therefore estopped from relying on any statute of limitations.

143. Defendants' fraudulent concealment is common to the Class and the two Subclasses.

IX. NAMED PLAINTIFF ALLEGATIONS.

A. The California Plaintiffs.

1. Plaintiff Misty Hong.

144. Plaintiff Misty Hong is currently a full-time college student. In or about March or April 2019, Ms. Hong downloaded the TikTok app onto her mobile device. At the time Ms. Hong downloaded the TikTok app, she did not read any privacy policy or terms of use, nor did she see discernible hyperlinks to or warnings about these items. In fact, she never clicked the sign-up button and never knowingly created an account with Defendants. However, months later, she discovered for the first time that Defendant TikTok, Inc. had created an account for her, without her knowledge or consent, and provided her with a user name (the word "user" followed by a combination of numbers followed by "@" followed by the word "user" followed by a combination of letters and numbers) and assigned her phone number as the account password.

145. Shortly after completing the download of the TikTok app onto her mobile device, Ms. Hong made approximately five or six videos using the TikTok app on her mobile device. Images of her face were captured in some or all of these videos. Ms. Hong experienced difficulty in timing the background music to lip-syncing and dancing. Consequently, after shooting each video, Ms. Hong (i) sometimes pressed the "next" button and (ii) sometimes pressed the "x" button and then the "reshoot" button. Ms. Hong neither saved nor posted any of these videos. But, as a result of sometimes pressing the "next" button, Defendants took some of these Private Videos without Ms. Hong's knowledge or consent. Images of Ms. Hong's face also have been captured in Musical.ly and/or TikTok videos recorded and posted by others.

146. During the time that the TikTok app was installed on Ms. Hong's mobile device, Defendants surreptitiously performed the following actions without notice to or the knowledge and consent of Ms. Hong: (i) Defendants took her User/Device Identifiers and Private Videos from her mobile device; (ii) Defendants took her biometric identifiers and information (including face geometry scans and voiceprints) from her and her friends'

mobile device and/or videos; (iii) Defendants took her private and personally-identifiable data and content from her mobile device before she had the opportunity to sign up and create an account; (iv) Defendants took her private and personally-identifiable data and content from her mobile device after she closed the TikTok app; and (v) Defendants transferred some or all such stolen data and content to servers located in China – including to servers under the control of third-parties who cooperate with the Chinese government.

147. Defendants performed these acts for the purpose of secretly collecting Ms. Hong's private and personally-identifiable data and content – including her User/Device Identifiers, biometric identifiers and information, and Private Videos – and using such data and content to track, profile and target Ms. Hong with advertisements. Further, Defendants have used Ms. Hong's private and personally-identifiable data and content for the purpose of developing their artificial intelligence capabilities and patenting commercially-valuable technologies. Defendants and others now have access to a living and information-laden dossier on Ms. Hong that can be used for further commercial advantage and other harmful purposes. Defendants have profited, and will continue to profit, from these activities.

148. Meanwhile, Ms. Hong has incurred harm as a result of Defendants' invasion of her privacy rights through their covert taking of her private and personally-identifiable data and content – including her User/Device Identifiers, biometric identifiers and information, and Private Videos. Ms. Hong also has suffered harm because Defendant's actions have diminished the value of her private and personally-identifiable data and content. Moreover, Ms. Hong has suffered injury to her mobile device. The battery, memory, CPU and bandwidth of her device has been compromised, and as a result the functioning of that device has been impaired and slowed, due to Defendants' clandestine and unlawful activities. Finally, Ms. Hong has incurred additional data usage and electricity costs that she would not have incurred but for Defendants' covert and unlawful actions.

2. Plaintiff A.S.

149. Plaintiff A.S., a minor who is currently 15 years old, first downloaded the

Musical.ly app to her mobile device and created a user account in 2016 when she was under age 13. She subsequently downloaded the Musical.ly app in 2017 to a new mobile device that was hers. In 2019, A.S. downloaded the TikTok app to another new mobile device that was hers. A.S. and her legal guardian have never seen or read any of Defendants' privacy policies or terms of use.

150. Beginning in 2016, A.S. created numerous videos using the Musical.ly app and the TikTok app. Many are Private Videos containing images of her face, while many others are videos containing her voice and images of her face that she intentionally uploaded and posted. A.S. used the augmented reality features and facial filters on her face in both Private Videos and in videos that she intentionally uploaded and posted.

151. During the time that the TikTok app was installed on A.S.'s mobile devices, Defendants surreptitiously performed the following actions without notice to or the knowledge and consent of A.S. or her legal guardian: (i) Defendants took her User/Device Identifiers, Private Videos and Private Video Images from her mobile devices; (ii) Defendants took her biometric identifiers and information (including face geometry scans and voiceprints) from her mobile devices and/or videos; (iii) Defendants took her private and personally-identifiable data and content from her other social media accounts; (iv) Defendants took her private and personally-identifiable data and content from her mobile devices before she had the opportunity to sign up and create an account; (v) Defendants took her private and personally-identifiable data and content from her mobile devices after she closed the TikTok app; and (vi) Defendants transferred some or all such stolen data and content to servers located in China – including to servers under the control of third-parties who cooperate with the Chinese government.

152. Defendants performed these acts for the purpose of secretly collecting A.S.'s private and personally-identifiable data and content – including her User/Device Identifiers, biometric identifiers and information, Private Videos and Private Video Images – and using such data and content to track, profile and target A.S. with advertisements. Further, Defendants have used A.S.'s private and personally-identifiable data and content

for the purpose of developing their artificial intelligence capabilities and patenting commercially-valuable technologies. Defendants and others now have access to a living and information-laden dossier on A.S. that can be used for further commercial advantage and other harmful purposes. Defendants have profited, and will continue to profit, from these activities.

153. Meanwhile, A.S. has incurred harm as a result of Defendants' invasion of her privacy rights through their covert taking of her private and personally-identifiable data and content – including her User/Device Identifiers, biometric identifiers and information, Private Videos and Private Video Images. A.S. also has suffered harm because Defendant's actions have diminished the value of her private and personally-identifiable data and content. Moreover, A.S. has suffered injury to her mobile devices. The battery, memory, CPU and bandwidth of such devices have been compromised, and as a result the functioning of those devices has been impaired and slowed, due to Defendants' clandestine and unlawful activities. Finally, A.S. has incurred additional data usage and electricity costs that she would not have incurred but for Defendants' covert and unlawful actions.

3. Plaintiff A.R.

154. A.R. downloaded the Musical.ly app to her mobile device and created a user account in or about 2017 when she was approximately 12 years old. Subsequently, in 2019, while still a minor, A.R. downloaded the TikTok app to a new mobile device that was hers. A.R. and her legal guardian have never seen or read any of Defendants' privacy policies or terms of use.

155. A.R. created numerous videos using the Musical.ly app and the TikTok app. Many are Private Videos containing images of her face, while many others are videos containing images of her face that she intentionally uploaded and posted. A.R. used the augmented reality features and facial filters on her face in her Private Videos. A.R.'s voice and images of A.R.'s face have been captured in Private Videos recorded by others, as well as in videos that were recorded, uploaded and posted by others.

156. During the time that the TikTok app was installed on A.R.'s mobile devices,

Defendants surreptitiously performed the following actions without notice to or the knowledge and consent of A.R. or her legal guardian: (i) Defendants took her User/Device Identifiers, Private Videos and Private Video Images from her mobile devices; (ii) Defendants took her biometric identifiers and information (including face geometry scans and voiceprints) from her and her friends' mobile devices and/or videos; (iii) Defendants took her private and personally-identifiable data and content from her mobile devices before she had the opportunity to sign up and create an account; (iv) Defendants took her private and personally-identifiable data and content from her mobile devices after she closed the TikTok app; and (v) Defendants transferred some or all such stolen data and content to servers located in China – including to servers under the control of third-parties who cooperate with the Chinese government.

157. Defendants performed these acts for the purpose of secretly collecting A.R.'s private and personally-identifiable data and content – including her User/Device Identifiers, biometric identifiers and information, Private Videos and Private Video Images – and using such data and content to track, profile and target A.R. with advertisements. Further, Defendants have used A.R.'s private and personally-identifiable data and content for the purpose of developing their artificial intelligence capabilities and patenting commercially-valuable technologies. Defendants and others now have access to a living and information-laden dossier on A.R. that can be used for further commercial advantage and other harmful purposes. Defendants have profited, and will continue to profit, from these activities.

158. Meanwhile, A.R. has incurred harm as a result of Defendants' invasion of her privacy rights through their covert taking of her private and personally-identifiable data and content – including her User/Device Identifiers, biometric identifiers and information, Private Videos and Private Video Images. A.R. also has suffered harm because Defendant's actions have diminished the value of her private and personally-identifiable data and content. Moreover, A.R. has suffered injury to her mobile devices. The battery, memory, CPU and bandwidth of her devices have been compromised, and as a result the

functioning of those devices has been impaired and slowed, due to Defendants' clandestine and unlawful activities. Finally, A.R. has incurred additional data usage and electricity costs that she would not have incurred but for Defendants' covert and unlawful actions.

B. The Illinois Plaintiffs.

1. Plaintiff Meghan Smith.

159. Plaintiff Meghan Smith downloaded the TikTok app to her mobile device and created a user account in 2018. Ms. Smith has never read and does not recall seeing any of Defendants' privacy policies or terms of use.

160. Ms. Smith created numerous videos using the TikTok app. Many are Private Videos containing her voice and images of her face, while many others are videos containing her voice and images of her face that she intentionally uploaded and posted. Ms. Smith used the augmented reality features and facial filters on her face in both Private Videos and in videos that she intentionally uploaded and posted.

161. During the time that the TikTok app was installed on Ms. Smith's mobile device, Defendants surreptitiously performed the following actions without notice to or the knowledge and consent of Ms. Smith: (i) Defendants took her User/Device Identifiers, Private Videos, and Private Video Images from her mobile device; (ii) Defendants took her biometric identifiers and information (including face geometry scans and voiceprints) from her mobile device and/or videos; (iii) Defendants took her private and personally-identifiable data and content from her mobile device before she had the opportunity to sign up and create an account; (iv) Defendants took her private and personally-identifiable data and content from her mobile device after she closed the TikTok app; and (v) Defendants transferred some or all such stolen data and content to servers located in China – including to servers under the control of third-parties who cooperate with the Chinese government.

162. Defendants performed these acts for the purpose of secretly collecting Ms. Smith's private and personally-identifiable data and content – including her User/Device Identifiers, biometric identifiers and information, Private Videos and Private Video Images – and using such data and content to track, profile and target Ms. Smith with

advertisements. Further, Defendants have used Ms. Smith's private and personally-identifiable data and content for the purpose of developing their artificial intelligence capabilities and patenting commercially-valuable technologies. Defendants and others now have access to a living and information-laden dossier on Ms. Smith that can be used for further commercial advantage and other harmful purposes. Defendants have profited, and will continue to profit, from these activities.

163. Meanwhile, Ms. Smith has incurred harm as a result of Defendants' invasion of her privacy rights through their covert taking of her private and personally-identifiable data and content – including her User/Device Identifiers, biometric identifiers and information, Private Videos and Private Video Images. Ms. Smith also has suffered harm because Defendant's actions have diminished the value of her private and personally-identifiable data and content. Moreover, Ms. Smith has suffered injury to her mobile device. The battery, memory, CPU and bandwidth of such device have been compromised, and as a result the functioning of that device has been impaired and slowed, due to Defendants' clandestine and unlawful activities. Finally, Ms. Smith has incurred additional data usage and electricity costs that she would not have incurred but for Defendants' covert and unlawful actions.

2. Plaintiffs C.W. and I.W.

164. Plaintiff C.W., a minor who is currently 11 years old, and Plaintiff I.W., a minor who is currently 8 years old, are siblings who each downloaded the TikTok app to their own mobile devices and created their respective user accounts in or about March 2019. C.W., I.W. and their legal guardian have never seen or read any of Defendants' privacy policies or terms of use.

165. C.W. and I.W. each created numerous videos using the TikTok app. Each has videos containing images of their respective faces that they intentionally uploaded and posted. C.W. and I.W. used the augmented reality features and facial filters on their respective faces in videos they intentionally uploaded and posted.

166. During the time that the TikTok app was installed on C.W.'s and I.W.'s

mobile devices, Defendants surreptitiously performed the following actions without notice to or the knowledge and consent of C.W., I.W., or their legal guardian: (i) Defendants took their User/Device Identifiers from their mobile devices; (ii) Defendants took their biometric identifiers and information (including face geometry scans and voiceprints) from their mobile device and/or videos; (iii) Defendants took their private and personally-identifiable data and content from their mobile devices before they had the opportunity to sign up and create an account; (iv) Defendants took their private and personally-identifiable data and content from their mobile devices after they closed the TikTok app; and (v) Defendants transferred some or all such stolen data and content to servers located in China – including to servers under the control of third-parties who cooperate with the Chinese government.

167. Defendants performed these acts for the purpose of secretly collecting C.W.'s and I.W.'s private and personally-identifiable data and content – including their User/Device Identifiers and biometric identifiers and information – and using such data and content to track, profile and target C.W. and I.W. with advertisements. Further, Defendants have used C.W.'s and I.W.'s private and personally-identifiable data and content for the purpose of developing Defendants' artificial intelligence capabilities and patenting commercially-valuable technologies. Defendants and others now have access to a living and information-laden dossier on C.W. and I.W. that can be used for further commercial advantage and other harmful purposes. Defendants have profited, and will continue to profit, from these activities.

168. Meanwhile, C.W. and I.W. have incurred harm as a result of Defendants' invasion of their privacy rights through Defendants' covert taking of C.W.'s and I.W.'s private and personally-identifiable data and content – including their User/Device Identifiers and biometric identifiers and information. C.W. and I.W. also have suffered harm because Defendant's actions have diminished the value of their private and personally-identifiable data and content. Moreover, C.W. and I.W. have suffered injury to their mobile devices. The battery, memory, CPU and bandwidth of such devices have been

compromised, and as a result the functioning of those devices has been impaired and slowed, due to Defendants' clandestine and unlawful activities. Finally, C.W. and I.W. have incurred additional data usage and electricity costs that they would not have incurred but for Defendants' covert and unlawful actions.

3. Plaintiff R.P.

169. R.P., a minor who is currently 11 years old, downloaded the TikTok app to her mobile device and created a user account in 2018. R.P. and her legal guardian have never seen or read any of Defendants' privacy policies or terms of use.

170. R.P. created numerous videos using the TikTok app. Many are Private Videos containing images of her face, while many others are videos containing images of her face that she intentionally uploaded and posted. R.P. used the augmented reality features and facial filters on her face in both Private Videos and in videos that she intentionally uploaded and posted. Images of R.P.'s face have been captured in videos that were recorded, uploaded and posted by others.

171. During the time that the TikTok app was installed on R.P.'s mobile device, Defendants surreptitiously performed the following actions without notice to or the knowledge and consent of R.P. or her legal guardian: (i) Defendants took her User/Device Identifiers, Private Videos and Private Video Images from her mobile device; (ii) Defendants took her biometric identifiers and information (including face geometry scans and voiceprints) from her mobile device and/or videos; (iii) Defendants took her private and personally-identifiable data and content from her mobile device before she had the opportunity to sign up and create an account; (iv) Defendants took her private and personally-identifiable data and content from her mobile device after she closed the TikTok app; and (v) Defendants transferred some or all such stolen data and content to servers located in China – including to servers under the control of third-parties who cooperate with the Chinese government.

172. Defendants performed these acts for the purpose of secretly collecting R.P.'s private and personally-identifiable data and content – including her User/Device

Identifiers, biometric identifiers and information, and Private Videos and Private Video Images – and using such data and content to track, profile and target R.P. with advertisements. Further, Defendants have used R.P.'s private and personally-identifiable data and content for the purpose of developing their artificial intelligence capabilities and patenting commercially-valuable technologies. Defendants and others now have access to a living and information-laden dossier on R.P. that can be used for further commercial advantage and other harmful purposes. Defendants have profited, and will continue to profit, from these activities.

173. Meanwhile, R.P. has incurred harm as a result of Defendants' invasion of her privacy rights through their covert taking of her private and personally-identifiable data and content – including her User/Device Identifiers, biometric identifiers and information, and Private Videos and Private Video Images. R.P. also has suffered harm because Defendant's actions have diminished the value of her private and personally-identifiable data and content. Moreover, R.P. has suffered injury to her mobile device. The battery, memory, CPU and bandwidth of her device have been compromised, and as a result the functioning of that device has been impaired and slowed, due to Defendants' clandestine and unlawful activities. Finally, R.P. has incurred additional data usage and electricity costs that she would not have incurred but for Defendants' covert and unlawful actions.

X. CLASS ALLEGATIONS.

174. Plaintiffs seek class certification of the class set forth herein pursuant to Federal Rule of Civil Procedure 23 ("Rule 23"). Specifically, Plaintiffs seek class certification of all claims for relief herein on behalf of a class and two subclasses defined as follows:

Class: All persons who used the TikTok app and/or the Musical.ly app on one or more of their mobile devices while residing in the United States.

California Subclass: All persons who used the TikTok app and/or the Musical.ly app on one or more of their mobile devices while residing in California.

Illinois Subclass: All persons who, while residing in Illinois, used the TikTok app

and/or the Musical.ly app on one or more of their mobile devices and who, while residing in Illinois, (i) used either app to make a video containing his or her own face and/or voice, and/or (ii) had his or her own face and/or voice captured in a video made by someone else with either app.

175. Plaintiffs are the proposed class representatives for the class. California Plaintiffs are the proposed class representatives for the California Subclass. Illinois Plaintiffs are the proposed class representatives for the Illinois Subclass.

176. Plaintiffs reserve the right to modify or refine the definitions of the Class and the two Subclasses based upon discovery of new information and in order to accommodate any of the Court's manageability concerns.

177. Excluded from the Class and the two Subclasses are: **(i)** any judge or magistrate judge presiding over this action and members of their staff, as well as members of their families; **(ii)** Defendants, Defendants' predecessors, parents, successors, heirs, assigns, subsidiaries, and any entity in which any Defendant or its parents have a controlling interest, as well as Defendants' current or former employees, agents, officers, and directors; **(iii)** persons who properly execute and file a timely request for exclusion from the class; **(iv)** persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; **(v)** counsel for Plaintiffs and Defendants; and **(vi)** the legal representatives, successors, and assigns of any such excluded persons.

178. **Ascertainability**. The proposed Class and Subclasses are readily ascertainable because they are defined using objective criteria so as to allow Class and Subclass members to determine if they are part of the Class and/or one of the two Subclasses. Further, the Class and two Subclasses can be readily identified through records maintained by Defendants.

179. **Numerosity (Rule 23(a)(1))**. The Class and two Subclasses are so numerous that joinder of individual members herein is impracticable. The exact number of Class and Subclass members, as herein identified and described, is not known, but download figures indicate that the TikTok app has been downloaded more than 120 million times in the

United States.

180. **Commonality (Rule 23(a)(2))**. Common questions of fact and law exist for each cause of action and predominate over questions affecting only individual Class and Subclass members, including the following:

a. Whether Defendants engaged in the activities and practices referenced above;

b. Whether Defendants' activities and practices referenced above constitute a violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030;

c. Whether Defendants' activities and practices referenced above constitute a violation of the California Comprehensive Data Access and Fraud Act, Cal. Pen. C. § 502;

d. Whether Defendants' activities and practices referenced above constitute a violation of the Right to Privacy under the California Constitution;

e. Whether Defendants' activities and practices referenced above constitute an intrusion upon seclusion;

f. Whether Defendants' activities and practices referenced above constitute a violation of the California Unfair Competition Law, Bus. & Prof. C. §§ 17200 *et seq*.

g. Whether Defendants' activities and practices referenced above constitute a violation of the California False Advertising Law, Bus. & Prof. C. §§ 17500 *et seq.*

h. Whether Defendants' activities and practices referenced above constitute negligence;

i. Whether Defendants' activities and practices referenced above constitute unjust enrichment concerning which restitution and/or disgorgement is warranted;

j. Whether Defendants' activities and practices referenced above constitute a violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et*

seq.;

k. Whether Plaintiffs and members of the Class and two Subclasses sustained damages as a result of Defendants' activities and practices referenced above, and, if so, in what amount;

l. Whether Defendants profited from their activities and practices referenced above, and, if so, in what amount;

m. What is the appropriate injunctive relief to ensure that Defendants no longer unlawfully: **(i)** take private and personally-identifiable TikTok user data and content – including User/Device Identifiers, biometric identifiers and information, and Private Videos and Private Video Images; **(ii)** utilize private and personally-identifiable TikTok user data and content to develop and patent commercially-valuable artificial intelligence technologies; **(iii)** utilize private and personally-identifiable TikTok user data and content to create consumer demand for and use of Defendants' other products; **(iv)** transfer such private and personally-identifiable TikTok user data and content to servers in China and to third parties either in China or whose data is accessible from within China; **(v)** cause the diminution in value of TikTok users' private and personally-identifiable data and content; **(vi)** cause injury and harm to TikTok users' mobile devices; **(vii)** cause TikTok users to incur higher data usage and electricity charges; **(viii)** retain the unlawfully assembled TikTok user dossiers, including all private and personally-identifiable data and content therein; and **(ix)** profile and target, based on the above activities, TikTok users with advertisements.

n. What is the appropriate injunctive relief to ensure that Defendants take reasonable measures to ensure that they and relevant third parties destroy unlawfully-acquired private and personally-identifiable TikTok user data and content in their possession, custody or control.

181. **Typicality (Rule 23(a)(3))**. Plaintiffs' claims are typical of the claims of members of the Class and two Subclasses because, among other things, Plaintiffs and members of the Class and two Subclasses sustained similar injuries as a result of

Defendants' uniform wrongful conduct and their legal claims all arise from the same events and wrongful conduct by Defendants.

182. **Adequacy (Rule 23(a)(4))**. Plaintiffs will fairly and adequately protect the interests of the Class and two Subclasses. Plaintiffs' interests do not conflict with the interests of the Class and Subclass members, and Plaintiffs have retained counsel experienced in complex class action and data privacy litigation to prosecute this case on behalf of the Class and two Subclasses.

183. **Predominance & Superiority (Rule 23(b)(3))**. In addition to satisfying the prerequisites of Rule 23(a), Plaintiffs satisfy the requirements for maintaining a class action under Rule 23(b)(3). Common questions of law and fact predominate over any questions affecting only individual Class and Subclass members, and a class action is superior to individual litigation and all other available methods for the fair and efficient adjudication of this controversy. The amount of damages available to Plaintiffs is insufficient to make litigation addressing Defendants' conduct economically feasible in the absence of the class action procedure. Individualized litigation also presents a potential for inconsistent or contradictory judgments, and increases the delay and expense presented by the complex legal and factual issues of the case to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

184. **Final Declaratory or Injunctive Relief (Rule 23(b)(2))**. Plaintiffs also satisfy the requirements for maintaining a class action under Rule 23(b)(2). Defendants have acted or refused to act on grounds that apply generally to the Class and two Subclasses, making final declaratory and/or injunctive relief appropriate with respect to the Class and two Subclasses as a whole.

185. **Particular Issues (Rule 23(c)(4))**. Plaintiffs also satisfy the requirements for maintaining a class action under Rule 23(c)(4). Their claims consist of particular issues that are common to all Class and Subclass members and are capable of class-wide

resolution that will significantly advance the litigation.

XI. CAUSES OF ACTION.

FIRST CAUSE OF ACTION

Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030

(On Behalf of the Plaintiffs and the Class)

186. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

187. The Plaintiffs' and the Class's mobile devices are, and at all relevant times have been, used for interstate communication and commerce, and are therefore "protected computers" under 18 U.S.C. § 1030(e)(2)(B).

188. Defendants have exceeded, and continue to exceed, authorized access to the Plaintiffs' and the Class's protected computers and obtained information thereby, in violation of 18 U.S.C. § 1030(a)(2), (a)(2)(C).

189. Defendants' conduct caused "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value" under 18 U.S.C. § 1030(c)(4)(A)(i)(I), *inter alia*, because of the secret transmission of the Plaintiffs' and the Class's private and personally-identifiable data and content – including User/Device Identifiers, biometric identifiers and information, and Private Videos and Private Video Images never intended for public consumption.

190. Defendants' conduct also constitutes "a threat to public health or safety" under 18 U.S.C. § 1030(c)(4)(A)(i)(IV), due to the private and personally-identifiable data and content of the Plaintiffs and the Class being made available to foreign actors, including foreign intelligence services, in locations without adequate legal privacy protections. That this threat is real and imminent is evidenced by the ban on the TikTok app instituted by the Defense Department, Navy, Army, Marines, Air Force, Coast Guard and Transportation Security Administration, as well as the proposed legislation by United States Senators that would ban federal employees from using the TikTok app. As Senators Schumer and Cotton wrote in an October 23, 2019 letter to the Acting Director of National Intelligence

concerning TikTok, "[s]ecurity experts have voiced concerns that China's vague patchwork of intelligence, national security, and cybersecurity laws compel Chinese companies to support and cooperate with intelligence work controlled by the Chinese Communist Party. Without an independent judiciary to review requests made by the Chinese government for data or other actions, there is no legal mechanism for Chinese companies to appeal if they disagree with a request."[134]

191. Accordingly, the Plaintiffs and the Class are entitled to "maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g).

SECOND CAUSE OF ACTION

Violation of the California Comprehensive

Data Access and Fraud Act, Cal. Pen. C. § 502

(On Behalf of the Plaintiffs and the Class)

192. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

193. Defendants' acts violate Cal. Pen. C. § 502(c)(1) because they have knowingly accessed, and continue to knowingly access, data and computers to wrongfully control or obtain data. The Plaintiffs' and the Class's private and personally-identifiable data and content accessed by Defendants – including the User/Device Identifiers, the biometric identifiers and information, and the Private Videos and Private Video Images never intended for public consumption – far exceeds any reasonable use of the Plaintiffs' and the Class's data and content to operate the TikTok app. There is no justification for Defendants' surreptitious collection and transfer of the Plaintiffs' and the Class's private and personally-identifiable data and content from their mobile devices and their other social media accounts; for Defendants' clandestine collection and transfer of the Plaintiffs'

[134] https://www.law360.com/articles/1213180/sens-want-tiktok-investigated-for-national-security-threats; https://www.cotton.senate.gov/?p=press_release&id=1239.

and the Class's private and personally-identifiable data and content before they even sign-up and create an account; for Defendants' covert collection and transfer of the Plaintiffs' and the Class's private and personally-identifiable data and content when the TikTok app is closed; or for Defendants having embedded source code within the TikTok app that transfers the Plaintiffs' and the Class's private and personally-identifiable data and content to servers and third-party companies based in China where such servers and third-party companies are subject to Chinese law requiring the sharing of such data and content with the Chinese government.

194. Defendants' acts violate Cal. Pen. C. § 502(c)(2) because they have knowingly accessed and without permission taken, copied, and made use of data from a computer – and they continue to do so. Defendants did not obtain permission to take, copy, and make use of the Plaintiffs' and the Class's private and personally-identifiable data and content – including the User/Device Identifiers, biometric identifiers and information, and Private Videos and Private Video Images never intended for public consumption – from their mobile devices and their other social media accounts. Nor did Defendants obtain permission to take, copy, and make use of the Plaintiffs' and the Class's private and personally-identifiable data and content from their mobile devices before they even sign-up and create an account. And Defendants did not obtain permission to take, copy, and make use of the Plaintiffs' and the Class's private and personally-identifiable data and content from their mobile devices when the TikTok app is closed. Finally, Defendants did not obtain permission to embed source code within the TikTok app that transfers the Plaintiffs' and the Class's private and personally-identifiable data and content to servers and third-party companies based in China where such servers and third-party companies are subject to Chinese law requiring the sharing of such data and content with the Chinese government.

195. Accordingly, the Plaintiffs and the Class are entitled to compensatory damages, including "any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was

or was not altered, damaged, or deleted by the access," injunctive relief, and attorneys' fees. Cal. Pen. C. § 502(e)(1), (2).

THIRD CAUSE OF ACTION

Violation of the Right to Privacy – California Constitution

(On Behalf of the California Plaintiffs and the California Subclass)

196. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

197. The California Plaintiffs and the California Subclass hold, and at all relevant times held, a legally protected privacy interest in their private and personally-identifiable data and content – including the User/Device Identifiers, the biometric identifiers and information, and the Private Videos and Private Video Images never intended for public consumption – on their mobile devices and in their other social media accounts that Defendants have taken.

198. There is a reasonable expectation of privacy concerning the California Plaintiffs' and the California Subclass's data and content under the circumstances present.

199. The reasonableness of the California Plaintiffs' and the California Subclass's expectation of privacy is supported by the undisclosed, hidden, and non-intuitive nature of Defendants' taking of private and personally-identifiable data and content – including the User/Device Identifiers, the biometric identifiers and information, and the Private Videos and Private Video Images never intended for public consumption – from the California Plaintiffs' and the California Subclass's mobile devices and other social media accounts.

200. Defendants' conduct constitutes and, at all relevant times, constituted a serious invasion of privacy, as Defendants either did not disclose at all, or failed to make an effective disclosure, that they would take and make use of – and allow third-party companies based in China to take and make use of – the California Plaintiffs' and the California Subclass's private and personally-identifiable data and content. Defendants intentionally invaded the California Plaintiffs' and the California Subclass's privacy interests by intentionally designing the TikTok app, including all associated code, to

surreptitiously obtain, improperly gain knowledge of, review, and retain their private and personally-identifiable data and content.

201. These intrusions are highly offensive to a reasonable person, as evidenced by substantial research, literature, and governmental enforcement and investigative efforts to protect consumer privacy against surreptitious technological intrusions. The offensiveness of Defendants' intrusion is heightened by Defendants' making the California Plaintiffs' and the California Subclass's private and personally-identifiable data and content available to third parties, including foreign governmental entities whose interests are opposed to those of United States citizens. The offensiveness of Defendants' intrusion is further heightened by Defendants' secret collection and transfer of the California Plaintiffs' and the California Subclass's private and personally-identifiable data and content before they even sign-up and create an account; by Defendants' covert collection and transfer of the California Plaintiffs' and the California Subclass's private and personally-identifiable data and content when the TikTok app is closed; and by Defendants' clandestine collection and transfer of the California Plaintiffs' and the California Subclass's private and personally-identifiable data and content from their other social media accounts. The intentionality of Defendants' conduct, and the steps they have taken to disguise and deny it, also demonstrate the highly offensive nature of their conduct. Further, Defendants' conduct targeted the California Plaintiffs' and the California Subclass's mobile devices, which the United States Supreme Court has characterized as almost a feature of human anatomy, and which contain the California Plaintiffs' and the California Subclass's private and personally-identifiable data and content.

202. The California Plaintiffs and the California Subclass were harmed by, and continue to suffer harm as a result of, the intrusion as detailed throughout this First Amended Complaint.

203. Defendants' conduct was a substantial factor in causing the harm suffered by the California Plaintiffs and the California Subclass.

204. The California Plaintiffs and the California Subclass seek nominal and

punitive damages as a result of Defendants' actions. Punitive damages are warranted because Defendants' malicious, oppressive, and willful actions were calculated to injure the California Plaintiffs and the California Subclass, and were made in conscious disregard of their rights. Punitive damages are also warranted to deter Defendants from engaging in future misconduct.

205. The California Plaintiffs and the California Subclass seek injunctive relief to rectify Defendants' actions, including but not limited to requiring Defendants to stop taking more private and personally-identifiable data and content of the California Plaintiffs and the California Subclass from their mobile devices and their other social media accounts than is reasonably necessary to operate the TikTok app; to make clear disclosures of the California Plaintiffs' and the California Subclass's private and personally-identifiable data and content that is reasonably necessary to operate the TikTok app; to obtain the California Plaintiffs' and the California Subclass's consent to the taking of their private and personally-identifiable data and content; to stop transferring the California Plaintiffs' and the California Subclass's private and personally-identifiable data and content to China, to servers located in China, or to servers or companies whose data is accessible from within China; and to recall and destroy the California Plaintiffs' and the California Subclass's private and personally-identifiable data and content already taken in contravention of the California Plaintiffs' and the California Subclass's right to privacy under the California Constitution.

206. The California Plaintiffs and the California Subclass seek restitution and disgorgement for Defendants' violation of their privacy rights. A person acting in conscious disregard of the rights of another is required to disgorge all profit because disgorgement both benefits the injured parties and deters the perpetrator from committing the same unlawful actions again. Disgorgement is available for conduct that constitutes "conscious interference with a claimant's legally protected interests," including tortious conduct or conduct that violates another duty or prohibition. Restatement (3rd) of Restitution and Unjust Enrichment, §§ 40, 44.

FOURTH CAUSE OF ACTION

Intrusion upon Seclusion

(On Behalf of the Plaintiffs and the Class)

207. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

208. "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." Restatement (2nd) of Torts § 652B.

209. The Plaintiffs and the Class have, and at all relevant times had, a reasonable expectation of privacy in their mobile devices and their other social media accounts, and their private affairs include their past, present and future activity on their mobile devices and their other social media accounts.

210. The reasonableness of the Plaintiffs' and the Class's expectations of privacy is supported by the undisclosed, hidden, and non-intuitive nature of Defendants' taking of private and personally-identifiable data and content from the Plaintiffs' and the Class's mobile devices and other social media accounts.

211. Defendants intentionally intruded upon the Plaintiffs' and the Class's solitude, seclusion, and private affairs – and continue to do so – by intentionally designing the TikTok app, including all associated code, to surreptitiously obtain, improperly gain knowledge of, review, and retain the Plaintiffs' and the Class's private and personally-identifiable data and content – including the User/Device Identifiers, the biometric identifiers and information, and the Private Videos and Private Video Images never intended for public consumption.

212. These intrusions are highly offensive to a reasonable person, as evidenced by substantial research, literature, and governmental enforcement and investigative efforts to protect consumer privacy against surreptitious technological intrusions. The offensiveness of Defendants' intrusion is heightened by Defendants' making the Plaintiffs' and the

Class's private and personally-identifiable data and content available to third parties, including foreign governmental entities whose interests are opposed to those of United States citizens. The offensiveness of Defendants' intrusion is further heightened by Defendants' secret collection and transfer of the Plaintiffs' and the Class's private and personally-identifiable data and content before they even sign-up and create an account; by Defendants' covert collection and transfer of the Plaintiffs' and the Class's private and personally-identifiable data and content when the TikTok app is closed; and by Defendants' clandestine collection and transfer of the Plaintiffs' and the Class's private and personally-identifiable data and content from their other social media accounts. The intentionality of Defendants' conduct, and the steps they have taken to disguise and deny it, also demonstrate the highly offensive nature of their conduct. Further, Defendants' conduct targeted the Plaintiffs' and the Class's mobile devices, which the United States Supreme Court has characterized as almost a feature of human anatomy, and which contain the Plaintiffs' and the Class's private and personally-identifiable data and content.

213. The Plaintiffs and the Class were harmed by, and continue to suffer harm as a result of, the intrusion as detailed throughout this First Amended Complaint.

214. Defendants' conduct was a substantial factor in causing the harm suffered by the Plaintiffs and the Class.

215. The Plaintiffs and the Class seek nominal and punitive damages as a result of Defendants' actions. Punitive damages are warranted because Defendants' malicious, oppressive, and willful actions were calculated to injure the Plaintiffs and the Class, and were made in conscious disregard of their rights. Punitive damages are also warranted to deter Defendants from engaging in future misconduct.

216. The Plaintiffs and the Class seek injunctive relief to rectify Defendants' actions, including but not limited to requiring Defendants to stop taking more private and personally-identifiable data and content from the Plaintiffs' and the Class's mobile devices and other social media accounts than is reasonably necessary to operate the TikTok app; to make clear disclosures of the Plaintiffs' and the Class's private and personally-identifiable

data and content that is reasonably necessary to operate the TikTok app; to obtain the Plaintiffs' and the Class's consent to the taking of such private and personally-identifiable data and content; to stop transferring the Plaintiffs' and the Class's private and personally-identifiable data and content to China, to servers located in China, or to servers or companies whose data is accessible from within China; and to recall and destroy the Plaintiffs' and the Class's private and personally-identifiable data and content already taken in contravention of the Plaintiffs' and the Class's privacy rights.

217. Plaintiffs and the Class seek restitution and disgorgement for Defendants' intrusion upon seclusion. A person acting in conscious disregard of the rights of another is required to disgorge all profit because disgorgement both benefits the injured parties and deters the perpetrator from committing the same unlawful actions again. Disgorgement is available for conduct that constitutes "conscious interference with a claimant's legally protected interests," including tortious conduct or conduct that violates another duty or prohibition. Restatement (3rd) of Restitution and Unjust Enrichment, §§ 40, 44.

FIFTH CAUSE OF ACTION

Violation of the California Unfair Competition Law,

Bus. & Prof. C. §§ 17200 et seq.

(On Behalf of the Plaintiffs and the Class)

218. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

219. The Unfair Competition Law, California Business & Professions Code §§ 17200, *et seq.* (the "UCL"), prohibits any "unlawful," "unfair," or "fraudulent" business act or practice, which can include false or misleading advertising.

220. Defendants violated, and continue to violate, the "unlawful" prong of the UCL through violation of statutes, constitutional provisions, and common law, as alleged herein.

221. Defendants violated, and continue to violate, the "unfair" prong of the UCL because they took private and personally-identifiable data and content – including the

User/Device Identifiers, the biometric identifiers and information, and the Private Videos and Private Video Images never intended for public consumption – from the Plaintiffs' and the Class's mobile devices and other social media accounts under circumstances in which the Plaintiffs and the Class would have no reason to know that such data and content was being taken.

222. The Plaintiffs and the Class had no reason to know because (i) there was no disclosure of Defendants' collection and transfer of the Plaintiffs' and the Class's biometric identifiers and information, Private Videos and Private Video Images not intended for public consumption; (ii) there was no disclosure of Defendants' collection and transfer of the Plaintiffs' and the Class's private and personally-identifiable data and content before they even sign-up and create an account; (iii) there was no disclosure of Defendants' collection and transfer of the Plaintiffs' and the Class's private and personally-identifiable data and content when the TikTok app is closed; (iv) there was no disclosure that Defendants had embedded source code within the TikTok app that transfers the Plaintiffs' and the Class's private and personally-identifiable data and content to servers and third-party companies based in China where such servers and third-party companies are subject to Chinese law requiring the sharing of such data and content with the Chinese government; and (v) there was no effective disclosure of the wide range of the private and personally-identifiable data and content, including User/Device Identifiers, that Defendants took from the Plaintiffs' and the Class's mobile devices and other social media accounts.

223. Defendants violated, and continue to violate, the "fraudulent" prong of the UCL because (i) Defendants made it appear that the Plaintiffs' and the Class's User/Device Identifiers, biometric identifiers and information, and Private Videos and Private Video Images would not be collected and transferred unless the Plaintiffs and the Class chose to do so, but in fact Defendants collected and transferred such data and content without notice or consent; (ii) Defendants made it appear that the Plaintiffs' and the Class's private and personally-identifiable data and content would not be collected and

transferred before they had signed-up and created an account, but in fact Defendants collected and transferred such data and content before sign-up and account creation without notice or consent; (iii) Defendants made it appear that the Plaintiffs' and the Class's private and personally-identifiable data and content would not be collected or transferred while the TikTok app is closed, but in fact Defendants clandestinely collected and transferred such data and content when the app was closed without notice or consent; (iv) Defendants made it appear that the Plaintiffs' and the Class's private and personally-identifiable data and content would not be transferred to servers and third-party companies based in China where such servers and third-party companies are subject to Chinese law requiring the sharing of such data and content with the Chinese government, but in fact Defendants covertly transferred such data and content to servers and third-party companies based in China without notice or consent; and (v) Defendants have intentionally refrained from disclosing the use to which the Plaintiffs' and the Class's private and personally-identifiable data and content has been put, while simultaneously providing misleading reassurances about Defendants' data collection and use practices. The Plaintiffs and the Class were misled by Defendants' concealment, and had no reason to believe that Defendants had taken the private and personally-identifiable data and content that they had taken.

224. The Plaintiffs and the Class have been harmed and have suffered economic injury as a result of Defendants' UCL violations. First, the Plaintiffs and the Class have suffered harm in the form of diminution of the value of their private and personally-identifiable data and content. Second, they have suffered harm to their mobile devices. The battery, memory, CPU and bandwidth of such devices have been compromised, and as a result the functioning of such devices has been impaired and slowed. Third, they have incurred additional data usage and electricity costs that they would not otherwise have incurred. Fourth, they have suffered harm as a result of the invasion of privacy stemming from Defendants' covert theft of their private and personally-identifiable data and content – including their User/Device Identifiers, biometric identifiers and information, and Private

Videos and Private Video Images.

225. Defendants, as a result of their conduct, have been able to reap unjust profits and revenues in violation of the UCL. This includes Defendants' profits and revenues from their targeted-advertising, improvements to their artificial intelligence technologies, their patent applications, and the increased consumer demand for and use of Defendants' other products. The Plaintiffs and the Class seek restitution and disgorgement of these unjust profits and revenues.

226. Unless restrained and enjoined, Defendants will continue to misrepresent their private and personally-identifiable data and content collection and use practices, and will not recall and destroy Plaintiffs' and the Class's wrongfully collected private and personally-identifiable data and content. Accordingly, injunctive relief is appropriate.

SIXTH CAUSE OF ACTION

Violation of the California False Advertising Law,

Bus. & Prof. C. §§ 17500 *et seq.*

(On Behalf of the Plaintiffs and the Class)

227. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

228. California's False Advertising Law (the "FAL") – Cal. Bus. & Prof. Code §§ 17500, *et seq.* – prohibits "any statement" that is "untrue or misleading" and made "with the intent directly or indirectly to dispose of" property or services.

229. Defendants' advertising is, and at all relevant times was, highly misleading. Defendants do not disclose at all, or do not meaningfully disclose, the private and personally-identifiable data and content – including the User/Device Identifiers, the biometric identifiers and information, and the Private Videos and Private Video Images never intended for public consumption – that they have collected and transferred from the Plaintiffs' and the Class's mobile devices and other social media accounts. Defendants also do not advertise that Defendants secretly take private and personally-identifiable data and content from the Plaintiffs' and the Class's mobile devices before they even sign up and

create an account, or that Defendants covertly take private and personally-identifiable data and content from the Plaintiffs' and the Class's mobile devices even when the TikTok app is closed. Nor do Defendants disclose that the Plaintiffs' and the Class's private and personally-identifiable data and content has been made available to foreign entities, including foreign government entities. As United States Senator Josh Hawley said on November 18, 2019: "If your child uses TikTok, there's a chance the Chinese Communist Party knows where they are, what they look like, what their voices sound like, and what they're watching" . . . "That's a feature TikTok doesn't advertise."[135]

230. Reasonable consumers, like the Plaintiffs and the Class, are – and at all relevant times were – likely to be misled by Defendants' misrepresentations. Reasonable consumers lack the means to verify Defendants' representations concerning their data and content collection and use practices, or to understand the fact or significance of Defendants' data and content collection and use practices.

231. The Plaintiffs and the Class have been harmed and have suffered economic injury as a result of Defendants' misrepresentations. First, they have suffered harm in the form of diminution of the value of their private and personally-identifiable data and content. Second, they have suffered harm to their mobile devices. The battery, memory, CPU and bandwidth of such devices have been compromised, and as a result the functioning of such devices has been impaired and slowed. Third, they have incurred additional data usage and electricity costs that they would not otherwise have incurred. Fourth, they have suffered harm as a result of the invasion of privacy stemming from Defendants' covert theft of their private and personally-identifiable data and content – including their User/Device Identifiers, biometric identifiers and information, and Private Videos and Private Video Images.

232. Defendants, as a result of their misrepresentations, have been able to reap

[135] https://www.law360.com/articles/1220783/no-more-data-storage-in-china-gop-senator-s-bill-says.

unjust profits and revenues. This includes Defendants' profits and revenues from their targeted-advertising, improvements to their artificial intelligence technologies, their patent applications, and the increased consumer demand for and use of Defendants' other products. The Plaintiffs and the Class seek restitution and disgorgement of these unjust profits and revenues.

233. Unless restrained and enjoined, Defendants will continue to misrepresent their private and personally-identifiable data and content collection and use practices, and will not recall and destroy Plaintiffs' and the Class's wrongfully collected private and personally-identifiable data and content. Accordingly, injunctive relief is appropriate.

SEVENTH CAUSE OF ACTION

Negligence

(On Behalf of the Plaintiffs and the Class)

234. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

235. The Plaintiffs and the Class entrusted Defendants with their private and personally-identifiable data and content – including the User/Device Identifiers, the biometric identifiers and information, and the Private Videos and Private Video Images never intended for public consumption. Defendants had a duty to handle that data and content with care due its sensitivity, and the expectation that such data and content would not be shared with third parties. This duty included Defendants' assurances that third-parties would not improperly collect or obtain such data and content, and Defendants' public statements, made in response to direct inquiries about the ability of China-based entities to access U.S. TikTok user data, that the Plaintiffs' and the Class's private and personally-identifiable data was not in fact subject to such access.

236. The Plaintiffs' and the Class's willingness to entrust Defendants with their private and personally-identifiable data and content was predicated on the understanding that Defendants would take appropriate measures to protect it. Defendants had a special relationship with the Plaintiffs and the Class as a result of being entrusted with their

private and personally-identifiable data and content, which provided an independent duty of care.

237. Defendants knew that the Plaintiffs' and the Class's private and personally-identifiable data and content had value, and Defendants have earned substantial revenues and profits as a result of collecting and using such private and personally-identifiable data and content. This includes Defendants' profits and revenues from their targeted-advertising, improvements to their artificial intelligence technologies, their patent applications, and the increased consumer demand for and use of Defendants' other products.

238. Defendants failed to use reasonable care to safeguard the Plaintiffs' and the Class's private and personally-identifiable data and content, giving third parties access to it without taking precautions to protect the Plaintiffs and the Class. Indeed, Defendants took no precautions at all, instead making the Plaintiffs' and the Class's private and personally-identifiable data and content directly available to third parties in jurisdictions with inadequate privacy protections, and in jurisdictions with inadequate constraints on governmental use of private and personally-identifiable data and content.

239. Defendants' failure to use care in allowing access to the Plaintiffs' and the Class's private and personally-identifiable data and content has caused foreseeable harm. Private and personally-identifiable data and content that can be used to track the physical movements and online activities of the Plaintiffs and the Class, and that is biometrically unique to each of the Plaintiffs and the members of the Class, has been transmitted to China-based companies, thereby exposing the Plaintiffs and the Class to a heightened, imminent risk of misuse, fraud, identity theft, Chinese government surveillance, and financial harm.

240. The Plaintiffs' and the Class's private and personally-identifiable data and content Defendants negligently allowed third parties to access allows such data and content to be aggregated with other data and content to identify, profile and target the Plaintiffs and the Class. As such, it is reasonable for the Plaintiffs and the Class to obtain identity

protection and credit monitoring services, and to recover the cost of these services from Defendants.

241. The injury to the Plaintiffs and the Class was a proximate, reasonably foreseeable result of Defendants' breaches of duty.

242. Defendants' conduct also constitutes gross negligence due to their extreme departure from ordinary standards of care, and their knowledge that they had failed to secure the Plaintiffs' and the Class's private and personally-identifiable data and content.

EIGHTH CAUSE OF ACTION

Restitution / Unjust Enrichment

(On Behalf of the Plaintiffs and the Class)

243. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

244. The Plaintiffs and the Class have conferred substantial benefits on Defendants by downloading and using the TikTok app. These include the Defendants' collection and use of the Plaintiffs' and the Class's private and personally-identifiable data and content – including their User/Device Identifiers, biometric identifiers and information, and Private Videos and Private Video Images never intended for public consumption. Such benefits also include the revenues and profits resulting from Defendants' collection and use of such data and content for Defendants' targeted-advertising, improvements to their artificial intelligence technologies, their patent applications, and the increased consumer demand for and use of Defendants' other products.

245. Defendants have knowingly and willingly accepted and enjoyed these benefits.

246. Defendants either knew or should have known that the benefits rendered by the Plaintiffs and the Class were given with the expectation that Defendants would not take and use the Plaintiffs' and the Class's private and personally-identifiable data and content that Defendants have taken and used without permission. For Defendants to retain the

aforementioned benefits under these circumstances is inequitable.

247. Through deliberate violation of the Plaintiffs' and the Class's privacy interests, and statutory and constitutional rights, Defendants each reaped benefits that resulted in each Defendant wrongfully receiving profits.

248. Equity demands disgorgement of Defendants' ill-gotten gains. Defendants will be unjustly enriched unless they are ordered to disgorge those profits for the benefit of the Plaintiffs and the Class.

249. As a direct and proximate result of Defendants' wrongful conduct and unjust enrichment, the Plaintiffs and the Class are entitled to restitution from Defendants and institution of a constructive trust disgorging all profits, benefits, and other compensation obtained by Defendants through this inequitable conduct.

NINTH CAUSE OF ACTION

Violation of Illinois's Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.*

(On Behalf of the Illinois Plaintiffs and the Illinois Subclass)

250. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

251. BIPA makes it unlawful for any private entity to, among other things, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it first: (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative." 740 ILCS 14/15(b).

252. Plaintiff Meghan Smith is, and at all relevant times was, an adult and resident of Illinois, and thus is, and at all relevant times was, a "person" and/or a "customer" within the meaning of BIPA. 740 ILCS 14/15(b). Plaintiff C.W. and Plaintiff

I.W. are, and at all relevant times were, minors and residents of Illinois, and thus are, and at all relevant times were, "persons" and/or "customers" as well. *Id.* Plaintiff C.W.'s and Plaintiff I.W.'s mother and legal guardian, Mikhaila Woodall, is Plaintiff C.W.'s and Plaintiff I.W.'s "legally authorized representative" within the meaning of BIPA, and served in such capacity at all times relevant to this action. *Id.* Plaintiff R.P. is, and at all relevant times was, a minor and resident of Illinois, and thus is, and at all relevant times was, a "person" and/or "customer" as well. *Id.* Plaintiff R.P.'s mother and legal guardian, Lynn Pavalon, is Plaintiff R.P.'s "legally authorized representative" within the meaning of BIPA, and served in such capacity at all times relevant to this action. *Id.*

253. Each Defendant is, and at all relevant times was, a "corporation, limited liability company, association, or other group, however organized," and thus is, and at all relevant times was, a "private entity" under the BIPA. 740 ILCS 14/10.

254. The Illinois Plaintiffs and the Illinois Subclass had their "biometric identifiers," including their face geometry scans and voiceprints, as well as their "biometric information" collected, captured, received, or otherwise obtained by Defendants as a result of the Illinois Plaintiffs' and the Illinois Subclass's use of the TikTok app. 740 ILCS 14/10.

255. At all relevant times, Defendants systematically and surreptitiously collected, captured, received or otherwise obtained the Illinois Plaintiffs' and the Illinois Subclass's "biometric identifiers" and "biometric information" without first obtaining signed written releases, as required by 740 ILCS 14/15(b)(3), from any of them or their "legally authorized representatives."

256. In fact, Defendants failed to properly inform the Illinois Plaintiffs and the Illinois Subclass, or any of their parents, legal guardians, or other "legally authorized representatives," in writing (or in any other way) that the Illinois Plaintiffs' and the Illinois Subclass's "biometric identifiers" and "biometric information" were being "collected or stored" by Defendants. Nor did Defendants inform the Illinois Plaintiffs and the Illinois Subclass, or any of their parents, legal guardians, or other "legally authorized

representatives," in writing of the specific purpose and length of term for which the Illinois Plaintiffs' and the Illinois Subclass's "biometric identifiers" and "biometric information" were being "collected, stored and used" as required by 740 ILCS 14/15(b)(1)-(2).

257. BIPA also makes it unlawful for a private entity "in possession of a biometric identifier or biometric information" to "sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information." 740 ILCS 14/15(c).

258. Defendants are, and at all relevant times were, "in possession of" the Illinois Plaintiffs' and the Illinois Subclass's "biometric identifiers," including but not limited to their face geometry scans and voiceprints, and "biometric information." Defendants profited from such "biometric identifiers" and "biometric information" by using them for targeted advertising, improvements to Defendants' artificial intelligence technologies, Defendants' patent applications, and the generation of increased demand for and use of Defendants' other products. 740 ILCS 14/15(c).

259. Finally, BIPA prohibits private entities "in possession of a biometric identifier or biometric information" from "disclos[ing], redisclos[ing], or otherwise disseminat[ing] a person's or a customer's biometric identifier or biometric information unless" any one of four enumerated conditions are met. 740 ILCS 14/15(d)(1)-(4). None of such conditions are met here.

260. Defendants disclose, redisclose and disseminate, and at all relevant times disclosed, redisclosed and disseminated, the Illinois Plaintiffs' and the Illinois Subclass's "biometric identifiers," including but not limited to their face geometry scans and voiceprints, and "biometric information" without the consent of any of them or their "legally authorized representatives." 740 ILCS 14/15(d)(1). Moreover, the disclosures and redisclosures did not "complete[] a financial transaction requested or authorized by" the Illinois Plaintiffs, the Illinois Subclass or any of their legally authorized representatives. 740 ILCS 14/15(d)(2). Nor are, or at any relevant times were, the disclosures and redisclosures "required by State or federal law or municipal ordinance." 740 ILCS

14/15(d)(3). Finally, at no point in time were the disclosures ever "required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction." 740 ILCS 14/15(d)(4).

261. BIPA mandates that a private entity "in possession of biometric identifiers or biometric information" "develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first." 740 ILCS 14/15(a).

262. But Defendants do not publicly provide any written policy establishing any retention schedule or guidelines for permanently destroying the Illinois Plaintiffs' and the Illinois Subclass's "biometric identifiers" and "biometric information." 740 ILCS 14/15(a).

263. BIPA also commands private entities "in possession of a biometric identifier or biometric information" to: (1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and (2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits and protects other confidential and sensitive information. 740 ILCS 14/15(e). Based on the facts alleged herein, including Defendants' lack of a public written policy, their failure to inform TikTok users that Defendants obtain such users' "biometric identifiers" and "biometric information," their failure to obtain written consent to collect or otherwise obtain TikTok users' "biometric identifiers" and "biometric information," and their unauthorized dissemination of TikTok users' "biometric identifiers" and "biometric information," Defendants have violated this provision too.

264. Defendants recklessly or intentionally violated each of BIPA's requirements and infringed the Illinois Plaintiffs' and the Illinois Subclass's rights to keep their immutable and uniquely identifying biometric identifiers and biometric information

private. As individuals subjected to each of Defendants' BIPA violations above, the Illinois Plaintiffs and the Illinois Subclass are and have been aggrieved. 740 ILCS 14/20.

265. On behalf of themselves and the Illinois Subclass, the Illinois Plaintiffs seek: (1) injunctive and equitable relief as is necessary to protect the interests of the Illinois Plaintiffs and the Illinois Subclass by requiring Defendants to comply with BIPA's requirements; (2) $1,000.00 or actual damages, whichever is greater, for each negligent violation of BIPA by Defendants; (3) $5,000.00 or actual damages, whichever is greater, for each intentional or reckless violation of BIPA by Defendants; and (4) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses. 740 ILCS 14/20(1)-(4).

XII. PRAYER FOR RELIEF.

WHEREFORE, Plaintiff respectfully requests relief against Defendants as set forth below:

(a) entry of an order certifying the proposed Class and Subclasses pursuant to Federal Rule of Civil Procedure 23;

(b) entry of an order appointing Plaintiffs as representatives of the Class and Subclasses;

(c) entry of an order appointing Plaintiffs' counsel as co-lead counsel for the Class and Subclasses;

(d) entry of an order for injunctive and declaratory relief as described herein, including but not limited to:

(i) enjoining Defendants, their affiliates, associates, officers, employees and agents from transmitting TikTok user data and content to China, to other locations or facilities where such TikTok user data and content is accessible from within China, and/or to anyone outside the defendant companies;

(ii) enjoining Defendants, their affiliates, associates, officers, employees and agents from taking TikTok users' private draft videos (including any frames, digital images or other content from such videos) and biometric identifiers and information

without advanced notice to, and the prior written consent of, such TikTok users or their legally authorized representatives (and, for the Illinois Subclass, without being in compliance with BIPA);

(iii) enjoining Defendants, their affiliates, associates, officers, employees and agents from taking physical/digital location tracking data, device ID data, personally-identifiable data and any other TikTok user data and content except that for which appropriate notice and consent is provided and which Defendants can show to be reasonably necessary for the lawful operation of the TikTok app within the United States;

(iv) mandating that Defendants, their affiliates, associates, officers, employees and agents recall and destroy the TikTok user data and content already taken in violation of law;

(v) mandating that Defendants, their affiliates, associates, officers, employees and agents remove from the TikTok app all SDKs based in China or whose data is otherwise accessible from within China;

(vi) mandating that Defendants, their affiliates, associates, officers, employees and agents implement protocols to ensure that no TikTok user data and content is transmitted to, or otherwise accessible from within, China;

(vii) mandating that Defendants, their affiliates, associates, officers, employees and agents hire third-party monitors for a period of at least three years to ensure that all of the above steps have been taken; and

(viii) mandating that Defendants, their affiliates, associates, officers, employees and agents provide written verifications on a quarterly basis to the court and counsel for the Plaintiffs in the form of a declaration under oath that the above steps have been satisfied.

(e) entry of judgment in favor of each Class and Subclass member for damages suffered as a result of the conduct alleged herein, punitive damages, restitution, and disgorgement, to include interest and prejudgment interest;

(f) award Plaintiff reasonable attorneys' fees and costs; and

(g) grant such other and further legal and equitable relief as the court deems just and equitable.

XIII. DEMAND FOR JURY TRIAL.

Plaintiffs demand a trial by jury on all issues so triable.

DATED: May 11, 2020

Ekwan E. Rhow - State Bar No. 174604
Dorothy Wolpert - State Bar No. 73213
Thomas R. Freeman - State Bar No. 135392
Marc E. Masters - State Bar No. 208375
BIRD, MARELLA, BOXER, WOLPERT, NESSIM, DROOKS, LINCENBERG & RHOW, P.C.
1875 Century Park East, 23rd Floor
Los Angeles, California 90067-2561
Telephone: (310) 201-2100
Facsimile: (310) 201-2110

By: */s/ Marc E. Masters*
Marc E. Masters

Attorneys for Plaintiffs Misty Hong, minor A.S., through her mother and legal guardian Laurel Slothower, and minor A.R., through her mother and legal guardian Gilda Avila

DATED: May 11, 2020

Marc L. Godino – State Bar No. 182689
Jonathan M. Rotter – State Bar No. 234137
Pavithra Rajesh – State Bar No. 323055
GLANCY PRONGAY & MURRAY LLP
1925 Century Park East, Suite 2100
Los Angeles, California 90067-2561
Telephone: (310) 201-9150
Email: info@glancylaw.com

By: */s/ Jonathan M. Rotter*
Jonathan M. Rotter

Attorneys for Plaintiffs Misty Hong, minor A.S., through her mother and legal guardian Laurel Slothower, and minor A.R., through her mother and legal guardian Gilda Avila

DATED: May 11, 2020

David M. Given – State Bar No. 142375
Nicholas A. Carlin – State Bar No. 112532
Brian S. Conlon – State Bar No. 303456
PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201
The Presidio
San Francisco, CA 94129
Telephone: (415) 398-0900
Email: dmg@phillaw.com

By: */s/ David M. Given*
David M. Given

Attorneys for Meghan Smith, minors C.W. and I.W., through their mother and legal guardian Mikhaila Woodall, and minor R.P., through her mother and legal guardian Lynn Pavalon

ATTESTATION

I, Jonathan M. Rotter, am the ECF user whose identification and password are being used to file this document. In compliance with Local Rule 5-1(i)(3), I hereby attest that each of the Signatories herein, concur in this filing.

DATED: May 11, 2020

s/ Jonathan M. Rotter
Jonathan M. Rotter

PROOF OF SERVICE BY ELECTRONIC POSTING

I, the undersigned say:

I am not a party to the above case and am over eighteen years old. On May 11, 2020, I served true and correct copies of the foregoing document, by posting the document electronically to the ECF website of the United States District Court for the Northern District of California, for receipt electronically by the parties listed on the Court's Service List.

I affirm under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on May 11, 2020, at Los Angeles, California.

s/ Jonathan M. Rotter
Jonathan M. Rotter